Protection from harm or more harm than good?

A critical evaluation of the PHOENIX Police National Computer application and concurrent police compliance with applicable data protection legislation

Christopher W. Baldwin

A thesis submitted in partial fulfilment of the requirements of the University of Sunderland for the degree of Doctor of Philosophy

July 2019

Table of Contents

Table of contents ..... **I**
Acknowledgements ..... **V**
Table of cases ..... **VI**
Table of statutes and other legislative instruments ..... **X**
List of common abbreviations and acronyms ..... **XIII**
Abstract ..... **XV**

Chapter 1: Introduction to the thesis **1**
1.1 Purpose of the thesis 1
1.2 Background to the research area 2
1.3 The four research questions 8
1.4 Originality of the research 13
1.5 Methodology 14
1.5.1 Why the Doctrinal approach will not work 14
1.5.2 Making the case for a (mostly) socio-legal approach 16
1.5.3 The Scotland 'comparison' 22
1.6 Conclusions 27

Chapter 2: The historical development of a national collection of criminal records in England and Wales **28**
2.1 Introduction 28
2.2 1730 – 1869: the embryonic collections 28
2.3 1869 – 1910: national statutory and police criminality data collation 32
2.4 The Criminal Records Office: the 'crooks clearinghouse' 42
2.5 James Rule's account of the CRO system 50
2.6 Conclusions 52

Chapter 3: PHOENIX **55**
3.1 Introduction 55
3.2 The Police National Computer 55
3.3 PHOENIX: the 'Criminal Justice Record System' 59
3.4 The PHOENIX criminality data: what the police are collating 62
3.4.1 Non-conviction data 62
3.4.2 Reprimands and Warnings 63

3.4.3 Cautions 65
3.4.4 Penalty Notice's for Disorder 70
3.4.5 Convictions 72
3.5 Conclusions 75

Chapter 4: The contemporary justifications for PHOENIX **78**
4.1 Introduction 78
4.2 The 'criminal records help to prevent crime' purpose 79
4.3 The 'criminal records help to detect offenders' purpose 85
4.4 The 'criminal records help to prosecute offenders' purpose 91
4.4.1 Pre-trial disclosure and bail applications 91
4.4.2 The use of PHOENIX data as 'bad character evidence' 93
4.4.3 Sentencing offenders 97
4.5 The (multitude) miscellaneous uses of criminal records 101
4.5.1 The ACRO Criminal Records Office 102
4.5.2 HM Prisons and Probation Service 104
4.5.3 Child protection and MAPPA 105
4.5.4 Other PHOENIX data utilisation 109
4.6 Conclusions 112

Chapter 5: The national collection of criminal records and compliance with the Data Protection Act 1984 ..... **113**
5.1 Introduction 113
5.2 Home Office resistance to Data Protection legislation 114
5.3 The Data Protection Act 1984 117
5.4 Police compliance with the fifth Data Principle 123
5.5 Police compliance with the eighth Data Principle 128
5.6 Conclusions 131

Chapter 6: Police compliance with the Data Protection Act 1998 in respect of the PHOENIX application **132**
6.1 Introduction 132
6.2 The Data Protection Act 1998 132
6.3 Police compliance with the first Data Principle 138
6.3.1 Unlawful arrests 138
6.3.2 Unlawful cautions 141

6.4 Police compliance with the fourth Data Principle 151
6.5 Police compliance with the seventh Data Principle 157
6.6 Conclusions 162

Chapter 7: The legality of the collection and retention of minor and inactive PHOENIX data **163**
7.1 Introduction 163
7.2 Weeding in the pre-data protection legislation period 164
7.3 Weeding during the DPA 1984 period 165
7.4 Weeding during the DPA 1998 period 169
7.5 *Bichard* and the first defeat of the Information Commissioner 172
7.6 The decisive second defeat of the Information Commissioner 181
7.7 The aftermath of the *Five Constables* decision 195
7.8 Conclusions 202

Chapter 8: Justifications for revisiting the decision in the *Five Constables* case **203**
8.1 Introduction 203
8.2 The criminal justice system does not require a complete record 203
8.3 The 'Ian Huntley myth' 204
8.4 Why indefinite retention might be considered 'excessive' 208
8.4.1 The back-record conversion programme was never completed 209
8.4.2 Scotland does not retain a complete collection 211
8.4.3 Recidivism studies support the deletion of old, inactive records 218
8.5 The deletion of certain records would solve the disclosure problem 232
8.6 Conclusions 241

Chapter 9: The scope for a European jurisprudential challenge to the *Five Constables* decision **242**
9.1 Introduction 242
9.2 The 'Right to Privacy' 242
9.3 Criminality data and Art.8: the decision in *MM* 243
9.4 The ECtHR rejection of unfettered police powers regarding the collation and storage of biometric criminality data 252
9.5 Does *S and Marper MM* apply only to the unconvicted? 258
9.6 The developing challenge to police hegemony on custody image data 262
9.7 Conclusions 274

Chapter 10: Summary of research findings and recommendations **275**
10.1 Introduction 275
10.2 Answering the first research question 275
10.3 Answering the second and third research questions 280
10.4 Answering the fourth research question 286
10.5 Looking to the LEDS and the LED: some concluding remarks 293

Bibliography **301**

Acknowledgements

There are so many people without whose help I would have been unable to complete this thesis and to whom I owe a debt of gratitude. The first of these is my Director of Studies, Dr. Karen Hadley. I consider myself extremely fortunate to have had my entire academic life shaped by such a superb academic and without her agreeing to be my Director of Studies, at a critical juncture in the research, I have little doubt that this thesis would not have been submitted. Karen has been supportive and attentive, ceaselessly reading drafts, annotating, critiquing and alternatively encouraging and cajoling as the situation demanded. One of the joys of undertaking this research has been to find that my sense of satisfaction at receiving positive feedback from her has not diminished whatsoever from the very earliest days of my undergraduate studies in 2003. My respect for Karen, as an intellect, an academic, a research supervisor and a person, remains undiminished and I have been proud to be her student once more. I only hope that I can be as good a supervisor to researchers in the future as she has been to me.

Due to various staffing rearrangements, I have had the benefit of co-supervision from too many exceptional academics to mention, and I express my gratitude to each of them for their guidance. Of these, I would like to particularly thank Dr. Ben Middleton, who always found time to read through my early drafts and provide valuable, critical comment and my current co-supervisor, Dr. Christopher J. Newman, whose experience and insight has constantly improved the work I was producing. I am extremely fortunate to have had such an exceptional scholar in my corner and I am eternally grateful for his assistance.

I consider myself extremely blessed to work in an extraordinarily supportive law department at the University of Sunderland filled, with limitlessly generous and immensely talented academics. To all of my colleagues and friends for their encouragement at various stages, for proof-reading chapters on a subject they have neither knowledge nor interest in, and for supplying sustenance when my strength began to sap – I thank you all.

This thesis would not have been drafted were it not for the support of my parents, whose lack of understanding of what this research entails is matched only by the depth of their pride that I have undertaken it. Their belief in me has never wavered, even when I tried my upmost during my formative years to bend and break it, and I hope that this thesis goes some way in validating the support they have always provided to me.

Finally, I take this opportunity to thank my wife, Natalie. It was she who alerted me to the potential data protection aspect of criminal record research, and without her pointing me to the rabbit hole, I would not have followed Alice into this particular wonderland. Quite simply, this thesis would not have been drafted but for her input and I will be eternally grateful to her for that. I hope that one day we can tell the story of how that happened to our daughter Elizabeth. It is to her that I dedicate this thesis. May you grow old and wise enough to choose not to read it.

Table of Authorities

Table of cases

Abraham v Commissioner of the Police of the Metropolis [2001] 1 WLR 1257

Al Fayed and others v. Commissioner of Police of the Metropolis [2004] EWCA Civ 1579

Blackburn v Commissioner of the Police for the Metropolis [1968] 2 QB 118

Caetano v Commissioner of Police of the Metropolis (2013) 177 JP 314

Catt v The United Kingdom, 24 January 2019 App. No. 43514/15

Chief Constable of Humberside Police and oths v The Information Commissioner [2009] EWCA Civ 1079

Criminal Practice Directions [2015] EWCA Crim 1567

Hill v the Chief Constable of West Yorkshire [1989] AC 53

MM v the United Kingdom [2012] ECHR 24029/07

Peruzzo v Germany (2013) 57 E.H.R.R SE17

Practice Direction (Criminal Law: Previous Convictions) [1955] 1 ALL ER 386

Practice Directions (Criminal Law: Practice: Particulars of Previous Convictions) [1966] 2 ALL ER 929

R (on the application of Catt) v Commissioner of Police of the Metropolis [2013] EWCA Civ 192

R (on the application of Catt) v Commissioner of Police of the Metropolis and another [2015] UKSC 9

R (on the application of F) and Thompson v the Secretary of State for the Home Department [2010] UKSC 17

R (on the application of Lee) v Chief Constable of Essex Police [2012] EWHC (Admin) 283

R (on the application of Manser) v Metropolitan Police Commissioner [2015] EWHC 3642 (Admin)

R (on the application of Mondelly) v Commissioner of Police for the Metropolis [2006] EWHC 2370

R (on the application of Murchison) v Southend Magistrates Court [2006] EWHC 569 (Admin)

R (on the application of R) v Durham Constabulary and another [2005] UKHL 21

R (on the application of RMC) v Metropolitan Police Commissioner [2012] EWHC 1681

R (on the application of S) v Chief Constable of South Yorkshire, R (on the application of Marper) v Chief Constable of South Yorkshire [2004] UKHL 39

R (on the application of Sisangia) v the Director of Legal Aid Casework [2016] EWCA Civ 24

R (on the application of Stratton) v Chief Constable of Thames Valley Police [2013] EWHC 1561

R (on the Application of T and another) v Sec. of State for the Home Department [2014] UKSC 35

R (on the application of W) v The Secretary of State for Justice [2015] EWHC Admin 1952

R (on the application of Wyman) v Chief Constable of Hampshire Constabulary [2006] EWHC 1904 (Admin)

R v Bryant [1978] 2 ALL ER 689

R v Chief Constable of B and another ex. Parte. R [1997] Lexis Citation 4824

R v Chief Constable of Kent and Another [1991] 93 Cr. App. R. 416

R v Chief Constable of North Wales ex. parte Thorpe [1998] 3 WLR 57

R v Commissioner of Police of the Metropolis ex parte P (1995) 160 JP 367

R v Commissioner of Police of the Metropolis, ex parte Thompson [1997] 1 WLR 1519

R v D (Attorney General's reference No.3/1999) [2001] 2 AC 91

R v Durham Constabulary ex. Parte R (FC) [2005] UKHL 21

R v Edwards [2006] 1 Cr App R 31

R v Evans [2016] EWCA Crim 31

R v Farinacci [1993] OJ No 2627 (QL)

R v Fouad Bennabou [2012] EWCA Crim 3088

R v Gellion [2006] EWCA Crim 281

R v Gore and Another [2009] ALL ER (D) 139 (Jul)

R v Hamer [2010] EWCA Crim 2053

R v Hardy [2007] EWCA Crim 760

R v Hunter and others [2016] ALL ER 1021

R v Huntley (Ian Kevin) [2005] EWHC 2083 (QB)

R v Keyte [1998] 2 Cr. App. R(S) 165

R v Minnis (Martyn David) [2012] EWCA Crim 461

R v Nazir [2003] EWCA Crim 901

R v Ngyuen [2008] EWCA Crim 585

R v Nourine [2013] EWCA Crim 73

R v O'Dowd [2009] 2 Cr App R 16

R v Queen (1981) 3 Cr.App.R (S.) 245

R v Rees [2000] ALL ER (D) 1481

R v Vasilou [2000] Crim. L.R. 845

R v Weir (26 May 2000) CA (Crim)

R v Worrel [2012] EWCA Crim 2657

R v Z [2000] 3 ALL ER 385

Re: Gallagher, R(P) and two others v Secretary of State for Justice [2019] UKSC 3

Re: Gaughran's Application for Judicial Review [2015] UKSC 29

*Re: KC's application for Judicial Review (*26 February 2016) (QBD)

Roy McGregor v John G McGlennan 1993 S.C.C.R 852

S and Marper v UK [2008] ECHR 30562/04

The Chief Constable of Humberside (and four others) v The Information Commissioner Information Tribunal Appeal Numbers EA/2007/0096, 98, 99, 108, 127 (21 July 2008)

The Chief Constables of West Yorkshire, South Yorkshire and North Wales Police v The Information Commissioner, The Information Tribunal, 12 October 2005

The Queen (on the Application of R) v The National Police Chiefs' Council and others [2017] EWHC 2586

The Queen v David Reginald Smith [2005] EWCA Crim 3244

W v Netherlands 20689/08, 20 January 2009

Woolmington v DPP [1935] AC 462

Table of statutes and other legislative instruments

Animal Welfare Act 2006

Anti-terrorism, Crime and Security Act 2001

Armed Forces Act 2006

Bail Act 1976

Children Act 2004

Children's Hearings (Scotland) Act 2011

Convention for the Protection of Human Rights and Fundamental Freedoms 1950

Council Framework Decision 2008/675/JHA, July 24 2008

County and Borough Police Act 1856

Crime and Disorder Act 1998

Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016

Criminal Justice Act 1982

Criminal Justice Act 2003

Criminal Justice and Courts Act 2015

Criminal Justice and Data Protection (Protocol No.36) Regulations 2014

Criminal Justice and Immigration Act 2008

Criminal Justice and Police Act 2001

Criminal Procedure (Scotland) Act 1995

Criminal Procedure and Investigations Act 1996

Criminal Procedure Rules 2015

Criminal Proceedings etc. (Reform) (Scotland) Act 2007

Data Protection Act 1984

Data Protection Act 1998

Data Protection Act 1998 (Commencement No. 4) Order 2015

Data Protection Act 2018

Directive 95/46/EC of the European Parliament and the Council of Europe (24 October 1995)

Explanatory Memorandum to Recommendation No. R (87) 15 (17 September 1987)

Forgery and Counterfeiting Act 1981

Freedom of Information Act 2000

General Data Protection Regulations 2016/679

Habitual Offenders Act 1869

Law Enforcement Directive 2016/680

Legal Aid, Sentencing and Punishment of Offenders Act 2012

Magistrates Courts Act 1980

Municipal Corporations Act 1835

National Police Records (Recordable Offences) (Amendment) Regulations 1997

National Police Records (Recordable Offences) (Amendment) Regulations 2003

National Police Records (Recordable Offences) (Amendment) Regulations 2005

National Police Records (Recordable Offences) (Amendment) Regulations 2007

National Police Records (Recordable Offences) (Amendment) Regulations 2012

National Police Records (Recordable Offences) (Amendment) Regulations 2016

National Police Records (Recordable Offences) Regulations 1985

National Police Records (Recordable Offences) Regulations 2000

Offences Against the Person Act 1861

Police Act 1996

Police Act 1997

Police Act 1997 (Criminal Records) Amendment Regulations 2007

Police Act 1997 (Criminal Records) Regulations 2002

Police and Criminal Evidence Act 1984

Police and Fire Reform (Scotland) Act 2012

Police National Records (Recordable Offences) (Amendment) Regulations 1989

Prevention of Crimes Act 1871

Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, Com (90) 314 SYN 287

Proposal for a Regulation of the European Parliament and the Council (COD, 2017/0444)

Protection of Freedoms Act 2012

Public Order Act 1986

Regulating the use of personal data in the police sector (Recommendation No. R (87) 15, 17 September 1987)

Rehabilitation of Offenders Act 1974

Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975

Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (Amendment) (England and Wales) Order 2013/1198

Road Traffic Act 1988

Scotland Act 1998

Serious Organised Crime and Police Act 2005

Sexual Offences Act 2003

Strasbourg Convention, European Treaty Series No.108

Theft Act 1968

List of commonly used abbreviations and acronyms

ACPO	Association of Chief Police Officers
ANPR	Automatic Number Plate Recognition
BCD	Biometric Criminality Data
CHS	Criminal History System
CPS	Crown Prosecution Service
CRB	Criminal Records Bureau
CRO	Criminal Records Office
CSO	Convict Supervision Office
DBS	Disclosure and Barring Service
DPA 1984	Data Protection Act 1984
DPA 1998	Data Protection Act 1998
FWS	The Final Warning Scheme
HCA 1869	Habitual Criminals Act 1869
HMIC	Her Majesty's Inspectorate of Constabularies
HMICFRS	Her Majesty's Inspectorate of Constabularies and the Fire and Rescue Service
ICO	Information Commissioner's Office
IDENT1	The National Fingerprint Database
IT	The Information Tribunal
LED	Law Enforcement Directive
LEDS	Law Enforcement Data Service
MAPPA	Multi-Agency Public Protection Arrangements
NDNAD	The National DNA Database
NFA	'No further action' disposal
NIB	National Identification Bureau
NLEDP	National Law Enforcement Data Programme

NPCC	National Police Chief's Council
NPIA	National Policing Improvement Agency
PACE 1984	Police and Criminal Evidence Act 1984
PHOENIX	Police Home Office Extended Names Index
PIA	Privacy Impact Assessment
PITO	Police Information Technology Organisation
PNC	Police National Computer
PND	Police National Database
PNfD	Penalty Notice for Disorder

Abstract

‘Big Data’ and the General Data Protection Regulations have been a prevailing feature of legal discourse in recent years, with interest in data protection law generally reaching a hitherto unprecedented pitch. Yet almost wholly outwith the parameters of current debate, the police in England and Wales are collating, storing and retaining on their Police National Computer data relating to offences and offenders (suspected or convicted) which now encompasses over twelve million citizens.

While there has been a growing acknowledgement of, and concurrent interest in, the legal and social ramifications of utilising this data for vetting purposes, research as to the actual data collation and retention process has itself been neglected almost entirely. Indeed, such is the over-reliance on presumption, and the general inattention paid to this area, that no-one even seems to have noticed that, despite the repeated use of the phrase ‘criminal record’, no authoritative definition of it exists, or that the police appear to have an effective *carte blanche* as to what data they can collate, how they store it and how long they retain it.

The purpose of this research is to address the deficits in the existing literature by asking four key questions; what data have the police been collating, are they acting concurrent with their Data Protection obligations regarding the collation and storage of the data and is the police retention of this data justiciable with regard to their stated purpose(s) for retaining it? It is the perhaps the last of these questions which perhaps invites the most multi-faceted debate. The police posit that an isolated conviction for theft recorded a decade or more previously is of ‘operational value’ to them in their crime detection and prevention duties. This research intends to critically examine that proposition, holding the police to account and asking whether there are questions for the police, and those supposedly charged with ensuring police data compliance, to answer.

1
Introduction to the thesis

1.1 Purpose of the thesis

The purpose of this thesis is to conduct an extensive, overarching and original analysis of the police collation, storage and retention of criminal records in England and Wales.

This analysis purports to identify in the first instance what criminality data is being collated, where it is being stored and for what duration. This will begin with a critical chronology aiming to identify and analyse the historical development of criminality data collation, tracking it from infancy to the modern, centralised collection. In essence, this is intended to establish what the collators of data have presumed to mean by the phrase 'criminal record'. The analysis will then move to systematise the police and criminal justice justifications for the collation and retention of the data, and to offer an evaluative commentary on whether the rationale commonly offered for the data retention justifies its collection.

The focus of the research will then diverge to provide a comprehensive evaluation and analysis of the current police practice of retaining criminality data against their concurrent statutory obligations under the applicable data protection legislation. This will be undertaken in three stages. The first is a critical inquiry into the provisions of the Data Protection Act 1984[1] ('the DPA 1984'), the processes by which criminal records data were held whilst that Act remained in force and the potential failings of the police in adhering to their obligations under it. The second is a fundamentally similar critical inquiry into the pertinent provisions of the Data Protection Act 1998[2] ('the DPA 1998'), collation processes during the applicable period and an identification of potential breaches of that legislation. The third stage involves a comprehensive examination of the police practices of criminality data retention, with especial focus on the nature of the data being retained and the timeframes involved with a view to evaluating whether these practices are consistent with

[1] 1984, ch.35
[2] 1998, ch.29

the data protection requirement of ensuring that data holdings not be 'excessive'[3] or 'for longer than is necessary' for the stipulated purpose(s).[4]

This final analysis will draw on recidivism studies, a brief comparative analysis with the retention policies for near identical data in Scotland, a more lengthy comparative analysis between retention of criminal records data and the concurrent application of legal principles to other types of criminality data retained in separate police databases and also the potential for a legal challenge to be brought in future on the basis that the present processes for retaining criminal records data runs contrary to, and arguably infringes, the Government's human rights obligations under the European Convention on Human Rights ('the ECHR')[5] to allow for recommendations for future reconsideration of present practice to be made.

1.2 Background to the research area

In 2017, when offering an analysis of the latest, in a seemingly now ceaseless, judicial challenge to the disclosure of a 'criminal record' for employment vetting purposes, Professor Liz Campbell opined that:

> Much judicial and academic ink has been spilled of late on the scheme governing the retention and use of personal data by the police and third parties such as employers. Of course, information relating to people's…criminal record is of significant operational value in detecting, tracking and resolving criminality'.[6]

With all due deference to the learned Professor, her statement is only partially accurate. As the next chapter of this thesis illustrates at length, the police in England and Wales certainly are the custodians of an enormous repository of personal data relating to crime and (suspected and convicted) criminals.[7] This has been so since broadly the middle of the nineteenth century when the various piecemeal local schemes for accumulating data with the intent of assisting area policing were replaced by a statutory obligation on the

[3] Ibid, sch.1, pt.I, s.3
[4] Ibid, sch.1, pt.I, s.5
[5] Formally titled 'The Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950'
[6] L. Campbell, 'Criminal Record and Human Rights' (2017) 9 Criminal Law Review 696
[7] Which is henceforth referred to simply as 'criminality data'. Such is the paucity of literature in this area that the author could not find an alternative definition to use in the undertaking of this research.

Metropolitan Police to retain data relating to certain types of offender[8] and today the police hold, on various systems, an enormous repository of data relating to millions of living citizens.

For example, the police hold a vast repository of fingerprint and DNA data[9] on those suspected of, cautioned, warned or reprimanded in respect of, or convicted of criminal offences.[10] On the National DNA Database ('NDNAD'), there are (at 31 March 2018) 6,196,278 subject profile records and 590,404 crime scene profile records[11] held by the Home Office who 'run [NDNAD] on behalf of UK police forces'.[12] The former involves the taking of an entire genome sample of every suspect the police arrest,[13] while the latter is DNA samples taken from crime scenes intended to be matched to the former to help track offenders.[14] According to the Home Office, this yields significant operational value to the police; between April 2001 and March 2018, it is claimed that 675,395 individual samples were matched to unsolved crimes.[15]

The taking of fingerprints from suspects and crime scenes was the brainchild of Sir Francis Galton and Sir Edward Henry, who trialled the technique in Bengal then brought it to Scotland Yard in 1901.[16] Today, IDENT1[17] is the 'National Fingerprint Database' and the repository for all electronic fingerprint scans taken from any suspect arrested[18] or from crime scenes themselves.[19] This is another vast repository of personal data; at March 2018, IDENT1 held 8,012,521 individual fingerprint records and 2,259,139 crime scene records.[20] Again, the system is 'operated by the Home Office' although the police 'own the data they enrol upon it' but, unlike NDNAD, the police have direct access to the system.[21] Unlike NDNAD, there is no attempt to quantify the 'results' produced by IDENT1, but

[8] See ch.2.4 of this research
[9] Referred to throughout this research collectively as 'biometric criminality data' or 'BCD'
[10] See ch.9.4 for a detailed examination of the legal parameters of what BCD is being collected, when and for how long it is now stored.
[11] National Police Chief's Council and the Home Office, 'National DNA Database Strategy Board Annual Report 2017/18' (February 2019) APS Group (HMSO) 10
[12] Ibid 9
[13] Ibid 7
[14] Ibid 8
[15] Ibid 7
[16] See ch.2.4 of this research
[17] Above n.11, 32
[18] Ibid
[19] Ibid 33
[20] Ibid 38
[21] Ibid 37

anecdotal examples abound as to its effectiveness[22] and indeed, despite some recent missteps, fingerprint evidence has become cornerstone of police criminal investigatory practice.[23]

Likewise, photographic images have been taken from those suspected, and convicted, of offences largely since the technology to do so has existed: such images[24] were being routinely collected by prisons as early as the 1780s and have formed part of the statutory police data holding since the 1860s.[25] Today, custody images are taken of all suspects arrested on suspicion of a criminal offence and are held on local police data systems before being uploaded (by all but nine police forces at February 2017) for use of all police officers in England and Wales onto the Police National Database ('the PND'). At July 2016, the PND held 19 million custody images.[26] Custody images 'are a standard feature of everyday policing', used to help identify suspects, offenders and witnesses[27] and are nowadays digitally searchable using facial recognition software.[28]

So far as this type of personal data is concerned, Professor Campbell's proposition holds true and the last fifteen years or so has indeed seen a proliferation of academic and judicial debate as to the legislative frameworks which govern the collation and retention of this data. This proliferation is evaluated at length, for comparative purposes, in chapter nine of this research and what emerges is that, so far as this type of personal criminality data is concerned, three correlating, if interdependent, tenets hold broadly true:

i. the subject matter is easily identifiable and well defined, and;

ii. the use of the subject matter is broadly uncontroversial (with the exception of facial recognition software for custody images, which has attracted some concern) with a general, and broadly evidentially based, presumption that such data has operational police use and, therefore;

[22] Ibid 35 – 36
[23] M. M. Houck, Forensic Fingerprints (Elsevier 2016) XV
[24] Now ordinarily referred to as 'custody images' (see Home Office, 'Review of the use and retention of custody images' (February 2017) 1) and henceforth so referred to throughout this research.
[25] Above n.16
[26] Home Office, 'Review of the use and retention of custody images' (February 2017) 2
[27] Ibid 1
[28] Ibid 19

iii. almost all of the academic debate, and judicial challenge, concerning this type of personal data has focused on the *collation* and *retention* of the data, rather than the *use* of it, with a particular focus on compliance with data protection legislation and human rights protections.

By contrast, very different tenets seem to apply to 'criminal records'. Indeed, 'criminal records' are themselves something of a nebulous concept: it is a phrase routinely (and perhaps lazily) used but incredibly difficult to define. Confusion abounds. In 1998, Uglow wrote of 'access to police and criminal records',[29] indicating surely the existence of both as separate entities, and spoke of 'a [central] collection of records of those who have committed recordable offences' while the police held 'information about non-recordable offences, cautions and a certain amount of intelligence in relation to suspected crimes'. The new PHOENIX application,[30] he surmised, would result in an amalgamation of these into one record collection.[31] How much of this might constitute a person's 'criminal record' was not made clear.

Uglow was not alone in struggling to identify the demarcation between a 'police record' and 'criminal record'. When the Shadow Home Secretary Anne Widdecombe told her party conference in 2000 that a new hard-line policy on 'soft' drugs would mean 'criminal records, rather than cautions', for perpetrators, she caused such confusion that she later tried to clarify that there would be a 'police record', but not a 'criminal record'. After finding that the intended 'clarification' merely obfuscated matters even further, Widdecombe conceded that 'the law is very confused about what a criminal record is'.[32]

Campbell, meanwhile writes of 'a complex and overlapping legislative framework governing the retention and disclosure of cautions, reprimands and convictions in particular'.[33] It must be presumed, therefore, that these are what she believes constitutes a 'criminal record'. Professor Terry Thomas, arguably one of the leading authorities on criminality data who has been publishing research into the collection, retention and use of

[29] S. Uglow, 'Criminal records under the Police Act 1997' (Apr. 1998) Criminal Law Review 235
[30] See ch.3 for a full examination of PHOENIX and the collection of record it contains.
[31] Above n.29, 236 – 7
[32] A. McSmith, 'No retreat on Tories' cannabis hard-line' *The Telegraph* (London, 7 October 2000) <https://www.telegraph.co.uk/news/uknews/1369256/No-retreat-on-Tories-cannabis-hard-line.html> accessed 13 May 2019
[33] Above n.6, 697

'criminal records' since the 1980s,[34] seems to suggest otherwise. Indeed, his seminal 2007 work on criminal records opens with the following proposition:

> The criminal courts impose sentences on people convicted of crime, and at the same time a record of that conviction and sentence is made. The criminal record thus created is the subject of this book.[35]

The approach, perhaps best considered as the 'traditional view' of the constituents of a 'criminal record, finds support from the Home Office[36] but it might be wondered whether Professor Thomas would stand by that definition today. As chapter two of this research first suggests,[37] and chapter three confirms, the criminality data held by the police certainly extends beyond a bare record of those convicted of offences in court; cautions, for example, while originally intended to deal informally with low-level and juvenile offending, were included in central records as early as 1995 at the suggestion of a Home Office Scrutiny Committee. Although not 'a court conviction', there are now considerable grounds for supposing that these form part of a 'criminal record'.[38]

Not only is there a dissonance between the existence of a uniform definition of 'criminal record' data as compared to the clear extant definitions for 'other' criminality data but there is also a considerable paradigm shift in the judicial and academic interest between each dataset. While the focus for custody images and BCD looks at legality of the *collection* and *retention* of the raw data, so far as 'criminal records' are concerned, the 'much academic ink' spilled has examined almost exclusively the *use* of the data itself. This has predominantly manifested itself in challenges to the disclosure of 'criminal records' for vetting purposes, which has transposed into public view the scale and volume of criminality data the police retain regarding individuals outwith the collection of court conviction data.[39]

---

[34] See, for example, T. Thomas, 'The Exchange of information between the police and social services departments' (1986) 8(4) Journal of Social Welfare and Family Law 215

[35] T. Thomas, 'Criminal Records: A Database for the Criminal Justice System and Beyond' (Palgrave MacMillan, 2007) 1

[36] Above n.32

[37] See ch.2.6 of this research; records of those acquitted of serious or sexual offences were being retained by some criminal record offices as early as 1970.

[38] See ch.4.4.3 of this research for a full examination of the caution record on PHOENIX.

[39] See ch.8.5 of this thesis for an examination of the use of 'criminal records' for employment vetting purposes, including an extrapolation of the data used for that purpose.

By contrast, there has been an almost complete dearth of ink spilled, judicial, academic or otherwise, into the *collation* and *retention* of 'criminal record' data itself. This is largely because the police have enjoyed an almost complete and unfettered hegemony on what they collect, where they store it and for how long for as long as they have held records.[40] There exists no express statutory framework, comparable to that for DNA or fingerprint data[41] or indeed at all, regulating criminal record data collection, storage and retention and there has been precisely one judicial challenge to the police hegemony.[42] At April 2019, neither the House of Lords nor the Supreme Court have yet to consider the issue as part of any judicial challenge.

This apparent neglect of interest is especially peculiar when it is noted that, since 1984, the police have had statutory obligations to manage their collection of criminal records in accordance with data protection legislation. Remarkably, this author can find almost no prior attempt to identify whether the police have fulfilled those obligations. Additionally, and in direct contrast to all other types of criminality data, the usefulness of the criminal record data for police operational purposes appears to be *presumed* and there is a rather self-evident paradox at the heart of such a presumption; how useful can a computerised record of court convictions really be in helping police to investigate an unsolved murder, for example?[43]

What emerges is that, so far as 'criminality data' is concerned, three tenets hold broadly true and should be contrasted to those for BCD and custody image data, namely that:

i. the subject matter is extremely difficult to identify and poorly defined, and

ii. the use of the subject matter is controversial with an apparently limited evidential basis for the usefulness of the data for police operational purposes, and;

iii. almost all of the academic debate, and judicial challenge, concerning this type of personal data has focused on the *use* of the data, rather than the *collation*

[40] This is discussed at length in chapters 3 and 7 of this research.
[41] Per s.63D of the Police and Criminal Evidence Act 1984, as discussed at ch.9.4 of this research.
[42] Chief Constable of Humberside Police and oths v The Information Commissioner [2009] EWCA Civ 1079
[43] This issue is discussed at length at various points of the research, particularly ch.4.2 – 4.3 and ch.8.4.

and retention of it, with a particular focus on compliance with data protection legislation and human rights protections.

It is against this backdrop that the research is being undertaken.

1.3 The four research questions

This research aims to address four key questions which have been neglected for so long by researchers in this area. These are as follows:

1. What is a 'criminal record'?

There is no statutory definition of 'criminal record'.[44] The first research question aims to remedy that lacuna by providing a contemporary definition of 'criminal record' which accurately reflects that which has been, and continues to be, 'recorded'.

The 'traditional view' is that a 'criminal record' is a formal record of court convictions and sentences. It is hypothesised, however, that this 'traditional view' will not be borne out by the research into what records are actually being kept, and that the research will in fact show that far more 'criminal' data is being, and has always been, 'recorded'.

The aim of chapters two and three, therefore, is to identify what 'criminal' data is being 'recorded. In the absence of any statutory guidance to the contrary, chapter two will commence by seeking to identify what 'criminal' data was being 'recorded' by those earliest protagonists engaged in that collation process. For the purposes of this research, the aim is to identify 'criminal' data where this is given it's adjectival dictionary meaning: 'that which has 'the character, or is the nature, of a crime'[45] while 'record' will be given its noun form, so that the research will identify that 'criminal data which is 'inscribed on a tangible medium and is retrievable in perceivable form'.[46] In this way, chapter two aims to provide a 'literal' definition of 'criminal record'.

[44] Above n.33. Perhaps the closest attempt comes in s.62 of the Criminal Justice and Data Protection (Protocol No.36) Regulations 2014/3141, which provides that a 'UK Criminal Record': '…in England and Wales [is] information in any form relating to convictions on a names database held by the secretary of state for the use of police forces generally'. This rather concurs with Thomas' 'traditional' definition.
[45] B. A. Garner, *Black's Law Dictionary* (9th edn, Thompson Reuters 2009) 430
[46] Ibid, 1387

As the research will show, in 1867 Parliament imposed a statutory obligation on the police to compile a central 'record' of 'Habitual Criminals'.[47] From that point forth, this thesis will focus attention on what criminality data was being collated pursuant to that (and those subsequent as enacted by later legislation) statutory obligation; by whom, where and how it was stored and for how long. The research will be guided by, but not limited to, the statutory obligations imposed; the research intends to determine whether the collections amassed met, or indeed exceeded, the statutory requirements.

Chapter two will chart this collation process throughout the history of the paper repositories of data collated by the Metropolitan Police and the Criminal Record Offices.[48] Chapter three will continue to chart the data collation exercise throughout the period of computerisation initiated by the implemented of the Police National Computer,[49] again identifying what criminality data is being 'recorded', how is it being recorded, by whom and for how long it is being retained. The third chapter will conclude by providing a detailed examination of the data currently being held on the PHOENIX application of the Police National Computer. This will allow the research to provide a comprehensive answer to the research question set.

2. In collating and storing criminal record data, did the police comply with the data principles contained in Schedule 1, Part I of the Data Protection Act 1984?

When American academic James Rule published an account of his observations of the operations and practices at the National Criminal Records Office at Scotland Yard in 1970, he claimed that the collection of records was so vast that it was almost impossible to retain a complete and accurate national 'criminal record',[50] while reports of unlawful access to the records were so rife that Lord Gardiner told the House of Lords in 1973 that private investigators were 'openly saying that they could anybody's criminal record for about £7'.[51]

[47] See ch.2.4 of this research.
[48] See ch.2.4 – 2.6 of this research.
[49] See ch.3.2 of this research.
[50] See ch.2.6 of this research.
[51] H.L Deb. 6 June 1973, vol.343, col.115

In light of these findings, and the entrenched resistance of both the Home Office and the police to the implementation of data protection legislation (both generally and in its potential application to the police), it is hypothesised that it is unlikely that the police will have adhered to the applicable Data Principles contained in Schedule 1, Part I of the DPA 1984.

There can be little question that the collection of criminal records constitutes 'personal data' for the purposes of the DPA 1984; the statute definition provides that 'personal data means data consisting of information which relates to a living individual who can be identified from that information'.[52] Reflecting the identifiable potential issues of concern, chapter five of this research will provide a critical evaluation of extant resource material with an especial focus on potential breaches of the fifth and eighth data principles; the requirement to ensure that data held be accurate and kept up to date[53] and that appropriate security measures be taken to ensure unauthorised access to personal data.[54]

3. In collating and storing criminal record data, did the police comply with the Data Principles contained in Schedule 1, Part I of the Data Protection Act 1998?

The enactment of the DPA 1998 imposed more stringent data obligations on police chiefs in respect of their criminal record data holdings. It is hypothesised that, if this research finds that the police were in breach of their obligations under the DPA 1984, then they are also likely to be in breach of their obligations under the later legislation.

The approach undertaken in chapter six, which aims to address directly this research question, is almost identical to that taken in chapter five. The research aims to identify extant reliable legal materials and to coalesce these into a critical narrative which examines at length potential breaches of the applicable Data Principles. As with chapter five, the foci is whether breaches have occurred in the collation and storage of the criminal records data, and a more 'broad brush' approach is taken in this chapter, however, with each principle being examined and evidence of potential breaches

[52] Per s.3 of the Data Protection Act 1984
[53] See chapter 5.4 of this research.
[54] See chapter 5.5 of this research.

highlighted as they arise (with the exception of Data Principles three and five, which are dealt with in later chapters).

4. Is the current regime for retention of criminal record data on the PHOENIX application 'excessive' and/or is the data being held for 'longer than is necessary' for its stipulated purpose?

This research question involves a detailed examination of whether the retention policy for criminal record data was compatible with the third and fifth DPA 1998 Data Principles respectively.

This research question takes its terms of reference from both the provisions of the DPA 1998 and the decision of the Court of Appeal in *Chief Constable of Humberside Police and oths. v The Information Commissioner.*[55] This case was the first, and to date only, consideration by an appellate court in England and Wales of whether the retention policies for criminal record data are compliant with the third and fifth Data Principles. The Court of Appeal held that the police were the ultimate arbiters of what data they needed for their operational purposes and that essentially was 'the end of the matter'.[56]

It is hypothesised that this approach is flawed in several respects. It is flawed because it accepts the police view of what is operationally valuable which does not appear to be supported by empirical evidence. It is flawed because it misinterprets the manner in which criminal record data is used for the various purposes cited by the court as justifications for a near indefinite retention period. It is also flawed because it is predicates that the collection and retention of criminal record data does not invoke Article 8 of the ECHR.

This research question is approached by evaluating each of the requisite elements in turn, with the particular focus throughout on minor and 'inactive' criminal record data. In chapter four, the research details the most common justifications ('or purposes') for the collection of criminal record data. These include those specifically cited by the Court of Appeal in *the Five Constables* case[57] as well as brief consideration of the other potential purposes which might be utilised in future to justify a lengthy retention of the

[55] Ibid n.42 and henceforth referred to as the 'Five Constables case'.
[56] Ibid [43]
[57] At ch.4.2 – 4.4 of this research.

data.[58] Each of these is considered in sufficient detail to ascertain whether the justifications stand scrutiny, assisted, where possible, by a consideration of academic and other extrinsic source material to substantiate the positions enunciated.

Chapter seven provides a substantive, critical analysis of the police retention policies up to, including, and subsequent to the decision in *the Five Constables* case. This is done by undertaking substantive primary and secondary legal research into the police policies *in situ* at each applicable point, critically analysing these policies to identify retention periods, trends and practices to identify and attempt to explain any inconsistencies in the approach taken by the police during their lengthy collection of records. It will also examine whether the police had put into practice their retention policies and whether the Court of Appeal pronouncement that the historic practice of deleting old and minor records was instituted for data protection reasons is accurate.

Chapter eight of this research aims to provide a critical re-evaluation of the decision in *the Five Constables* case and, specifically, the justifications provided by the police (and upheld by the Court) for the near indefinite retention of all criminality data on the PHOENIX application. This is done by examining in turn each of the key tenets of the police position; namely that the criminal justice system requires all data be collected,[59] that they are obligated to retain data because of the *Soham* murders[60] and that the data has critical use for their own operational purposes. A comparison with the record retention system in Scotland is offered, along with a detailed analysis of whether criminological studies into offending, propensity, recidivism and desistence supports the police contention that even very minor and inactive records aid them in the prevention and investigation of offences. It is intended to provide an evidence-based analysis of whether the decades of criminological, sociological and legal research into these areas supports, or disapproves, of that police proposition.[61]

Chapter nine of this research then moves to consider the proposition, stated in *the Five Constables* case, that Article 8 of the EHCR does not apply to the collection of criminal records data. This will involve a detailed, critical evaluation of pertinent primary legal source material, specifically the lead decision of the appellate courts in England and

[58] At ch.4.5 of this research.
[59] See ch.8.2 of this research.
[60] See ch.8.3 of this research.
[61] See ch.8.4 of this research.

Wales and the European Court of Human Rights to determine whether the position offered in *the Five Constables* in 2009 stands scrutiny today, and whether a new challenge might be successful utilising the ECHR where data protection legislation is insufficient for that purpose.

1.4 Originality of the research

The collection of criminal records has begun, in recent years, to draw significant academic attention, but almost the entirety of that attention has been focused on the *use* of criminal records, predominantly for employment vetting purposes.[62]

There is, so far as this author is aware, almost no extant research into the collection of records itself; what has been collected, where it is stored and why it is being used. This research, so far as is practicable, intends to eschew entirely an analysis of record *use* except to identify whether that use justifies the fact of collating and retaining the data itself. This focus is original and will add significantly to the body of existing research by undermining the seemingly widespread assumption that the data *must* be collated and retained as it is currently.

Originality also stems from each of the four research questions. As has been indicated, there is no legal or other universally accepted definition of 'criminal record'. This research will demonstrate precisely what is being recorded, where and for how long it is retained. In this regard, it intends to rectify the omission in the extant literature by offering a research-based definition of 'criminal record'. It will provide an analysis of whether the police have committed breaches of data protection legislation; an original analysis on the basis that such is entirely omitted from the existing literature.

Moreover, the attempt in this research to systematise the various justifications for the extensive retention of the data, to analyse these critically with direct reference to empirical studies and to then scrutinise the present position with direct reference to recent judicial authority is also original and will add, in this author's view, something of considerable importance to the extant debate on criminal records.

[62] See, for example, J. Grace, 'Old convictions never die, they just fade away: the permanency of convictions and cautions for criminal offences in the UK' (2014) 78(2) Journal of Criminal Law 121 and K. Jones, 'Disclosure of youth criminal records' (2018) 8 Archbold Review 6.

1.5 Methodology

Whilst perhaps once not considered as such, identifying an appropriate methodology is now (rightly) considered one of the 'core components' of legal research.[63] What follows is a discussion on potential methods of legal research pertinent to this thesis, and an analytical discussion of the methodology selected, along with the methods inherent to this and justifications provided for utilising these.

1.5.1 Why the Doctrinal approach will not work

Cahillane and Schweppe confirm that 'black-letter or doctrinal analysis' is at the heart of traditional legal research and method'.[64] It is, according to Salter and Mason:

> A research methodology that concentrates on seeking to provide a detailed and highly technical commentary upon, and systematic exposition of, the content of legal doctrine. This doctrine is interpreted as if it were a separate, independent and coherent 'system of rules'. The priority is to gather, organise and describe legal rules, and offer commentary upon the emergence and significance of the authoritative legal sources that these rules contain'.[65]

At its core, doctrinal legal research involves a search to identify 'what the law is in a particular area'.[66] This is done by 'using as raw materials the work of the legal system itself; constitutional documents, primary and secondary legislation and recorded court judgments'; the so-called 'primary' legal source materials.[67] Once these are identified, collated and analysed, doctrinal legal research will move to the collation and analysis of supplementary, relevant legal materials; journal articles and other written commentaries on the case law and legislation; the so-called 'secondary sources'. These will often be selected with a historical perspective, allowing for the compilation of a chronology of legal development. It is the synthesis of these materials, focusing on judicial reasoning and legislative enactment, that forms the embodiment of the doctrinal approach.[68]

---

[63] L. Cahillane and J. Schweppe, *Legal Research Methods: Principles and Practicalities* (Clarus Press 2016) 1 – 2
[64] Ibid, 21
[65] M. Salter and J. Mason, *Writing Law Dissertations* (Pearson Longman 2007) 49
[66] M. McConville and W. H. Chui, *Research Methods for Law* (2nd edn, Edinburgh University Press 2017) 20 – 21
[67] Above n.63, 23
[68] Above n.65, 21

The central purpose of 'black-letter' approach to legal research is to identify a series of legal rules by identifying and analysing a smaller subset of general legal principles.[69] The methodology 'can be seen as analogous to a social science literature review' in that it involves 'a systematic, explicit and reproducible method for identifying, evaluating and synthesising the existing body of completed and recorded work produced by researchers, scholars and practitioners'.[70] Although often appearing *prima facie* simplistic, doctrinal legal research is 'complex, multi-layered and distinctive'[71] and 'demanding, useful and satisfying work'.[72] It allows, as a basis, for the mapping of areas of law which have been previously unexplored.[73]

The author has elected not to follow a strictly doctrinal approach in the conducting of this research. This is for a number of reasons. The first is that, it is submitted, the first research question cannot be tackled in a doctrinal manner, as there exists no primary definition of 'criminal records' – indeed, it is this lacuna in the legal canon which gives rise to the desire to answer the first research question.

The remaining three research questions involve research and subsequent analysis which must reach beyond a purely doctrinal approach. This is because these will require;

i. an examination of not just the legal rules governing to the collation, storage and retention of data, and;

ii. a detailed critical analysis of *how* those legal rules apply to a specific collection of data held by a particular social institution, and;

iii. a subsequent critical analysis of whether the processes implemented by that institution are justiciable, with reference to particular social, economic and criminal justice factors.

[69] Above n.64, 44
[70] Above n.65, 25
[71] Above n.63, 21
[72] Ibid, 25
[73] Ibid

Such an approach therefore lends the research to a methodological approach (or approaches) outwith the doctrinal method. Even as regards the fourth research question, which *might* theoretically be tackled by a purely doctrinal approach,[74] there is an obvious incentive to move beyond the doctrinal approach. In the *Five Constables* case, when making their determination as to the appropriate retention period applicable for the PHOENIX data, the Court declared that:

> If the police say rationally and reasonably that convictions, however old or minor, have a value in the work they do that should, in effect, be the end of the matter. It is simply the honest and rationally held belief that convictions, however old and however minor, can be of value in the fight against crime and thus the retention of that information should not be denied to the police.[75]

This, it is submitted, is not a doctrinal approach. It is an approach which interprets the positive meaning of primary legislation by specific reference to the alleged operational requirements of a social organisation. It is a means of creating doctrine by reference to the manner in which the law operates, or at least, is claimed to operate. This lends itself to an alternative research methodology; that of the socio-legal researcher.

1.5.2 Making the case for a (mostly) socio-legal approach

The socio-legal method is difficult to define because of the depth and breadth of research conducted under its broad tent.[76] Some have attempted to narrow it's parameters,[77] but the modern consensus is that the socio-legal approach involves an examination of 'law in context';[78] that is to say, an examination of both the 'law in books' (as might concern the 'doctrinal' researcher) and 'law in action'[79] in order to provide an analysis of the law in its rightful context as a 'social phenomenon'[80] – the product of the

[74] Indeed, chapter nine of this research arguably provides an attempt to do this, albeit by analogous reference to European jurisprudence flowing from similar, related but different criminality data collections.
[75] Above n.42 [43]
[76] F. Cownie and A. Bradney, 'Socio-legal studies. A challenge to the doctrinal approach' in D. Watkins and M. Burton, *Research Methods in Law* (Routledge 2018) 42
[77] C.M Campbell and P. Wiles, 'The Study of Law and Society in Britain' (1976) 10(4) Law and Society Review 547, 548 – 9
[78] D. O'Donovan, 'Socio-Legal Methodology: Conceptual Underpinnings, Justification and Practical Pitfalls' in L. Cahillane and J. Schweppe, *Legal Research Methods: Principles and Practicalities* (Clarus Press 2016) 109
[79] Above n.66, 6
[80] Above n.76

influence of social forces and interests on internally constructed rules and process.[81] Allott summarises the socio-legal approach as being based upon the notion that:

> Law seems to have a special status among social phenomena by reason of its forms, it's rituals, it's specialised language, it's special rationality even, and even its specific social effects. But, on the other hand, law is clearly embedded in the totality of the social process which is its cause, and on which is has substantial determinative effect, not least in providing the continuing structure of society.[82]

The breadth of research conducted under the umbrella of 'socio-legal work' has led one researcher to claim that any legal research 'which lies outwith the internal perspective of doctrinal methodology' is properly considered socio-legal research.[83] Salter and Mason, meanwhile, assert that 'the meaning of socio-legal studies cannot be decided once and for all. This is because it largely depends upon types of activity carried out by those who identify themselves as contributors to this movement'.[84]

Socio-legal research is conducted because the researcher believes that while the language of the law has importance, that this cannot be considered in isolation from the interrelationship between the law and society, politics and morality.[85] It therefore follows that socio-legal research is an interdisciplinary endeavour, allowing the lawyer engaged in legal research which incorporates methods and materials from different disciplines, such as economics, politics, history, social sciences and the humanities.[86] Indeed, as Cownie and Bradney note:

> socio-legal studies has encompassed the use by academic lawyers of a very wide range of disciplines… it is now difficult to think of any discipline in the social sciences or the humanities that has not be used by scholars working in the socio-legal mode'.[87]

---

[81] Above n.65, 122
[82] P. Allott, *The Health of Nations: Society and Law Beyond the State* (Cambridge University Press 2002) 36
[83] C. McCrudden, 'Legal Research and the Social Sciences' (2006) 122 Law Quarterly Review 632
[84] Above n.81
[85] L. Lammasniemi, *Law Dissertations. A Step-by-Step Guide* (Routledge 2018) 74
[86] Economic and Social Research Council, 'Review of Socio-Legal Studies: Final Report' (Swindon, 1994) 1
[87] Above n.76, 43

Proponents of socio-legal research generally claim it to be an 'exciting, wide-ranging and varied area of research activity'[88] and 'the most important scholarship currently being undertaken in the legal world'.[89] Socio-legal research has emerged as a popular 'alternative' to doctrinal analysis; Cownie's research estimated that, by 2004, around half of research-active legal academics described themselves as being 'socio-legal researchers' while many of those who did not categorise themselves as such were actually engaged in work 'indistinguishable' from colleagues who did describe themselves as socio-legal researchers.[90]

Socio-legal research is useful because, according to Jolley, it allows for a critical analysis of the 'law in action'; a socio-legal researcher will concentrate not just on the law itself but will also conduct a 'close study of the actions (and omissions) of legal officials'.[91] Such an approach is well-suited to research of the kind undertaken in this thesis, where the focus to all four researcher questions lies largely with the activities of the police; specifically in their compilation of criminality data (the first research question) and their subsequent actions in collating, storing and retaining that data (the remaining research questions).

This type of socio-legal study aims to examine the 'gap' between the law in books and the way in which legal officials act in accordance with that law – that identified by Jolley as 'the significant difference between the legal form of a particular measure and it's actual effect and practical force'.[92] In the case of the second and third research questions particularly[93], this approach allows for the thesis to identify in the first instance what the 'legal form' is (the Data Protection legislation), then the manner in which the police have compiled, stored and retained criminality data before moving to identify the 'gap' as a means of attempting to answer those research questions. The first research question must, by necessity, take such an approach to address the lacuna in the 'books' where no legal definition of 'criminal records' exists.

The 'broad church' approach which is typical of socio-legal research may result in definitional difficulties, however, according to the Socio-legal Studies Association the

[88] Above n.85
[89] R. Cotterrell, *Law's Community: Legal Theory in Sociological Perspective* (Clarendon Press 1995) 314
[90] F. Cownie, *Legal Academics: Culture and Identities* (Hart Publishing 2004) 54 – 58
[91] S. Jolly, 'Family Law', in P. Thomas, *Socio-Legal Studies* (Ashgate-Dartmouth 1997) 343
[92] Ibid
[93] Chapters 5 – 6 of this thesis follow almost exclusively this approach.

question ‘what is socio-legal research’ can be answered by the identification of three principle strands of socio-legal research.[94] These are:

i. Higher level social theories of law disconnected from empirical studies;

ii. Theories developed in the middle-range that are ‘grounded’ in the findings of empirical research (and which in turn aim to prompt further empirical studies to test the validity of their theoretical claims);

iii. Policy driven projects that are entirely empirical.[95]

It is intended for this research to join the second of these three strands. In attempting to answer the second, third and fourth research questions, the author will attempt to make theoretical postulations based, or perhaps even ‘supported’, by the quantitative data predominantly made available by official government publications or by the empirical work of academics made available via peer-reviewed, published research.

In chapter three, for example, almost doctrinal exposition and analysis of what is contained on the PHOENIX database is interwoven with empirical data to make analytical evaluations of the material contained in that database as a means of working towards answering the first research question. Chapters five and six draw together data provided by Governmental statistics to identify potential ‘defects’ in the police implementation of the various Data Protection Principles, while chapter eight particular aims to tackle the fourth research question by reference to various theoretical positions regarding the ‘operational usefulness’ of criminality data which are supported, where possible, by empirical data obtained either in official sources of from previous academic research.

According to Bradney and Cownie, the socio-legal researcher ‘must be prepared to use a far wider range of sources in both paper and electronic formats than would be the case for a black-letter project’.[96] While the doctrinal researcher is primarily concerned

[94] Above n.65, 122 – 3
[95] B. Hutter and S. Lloyd-Bostock, ‘The Interdependence of Theory, Empirical Work and Social Relevance in Socio-Legal Studies’ in K. Hawkins (ed) *The Human Face of Law: Essays in Honour of Donald Harris* (Oxford University Press 1997) 23
[96] F. Cowney and A. Bradney, *Teaching Legal System* (1999), in M. Salter and J. Mason, *Writing Law Dissertations* (Pearson Longman 2007) 129 – 30

with the primary and secondary legal source materials, the socio-legal researcher uses these as the 'legal' grounding of the work but will also seek to 'often draw from source materials that are not purely legal, and from other disciplines.[97] Lammasniemi claims that the common research materials of the socio-legal researcher include; statutes, secondary legislation, case law, reports from Government, non-governmental organisations and other stakeholder organisations, academic scholarship from law and other disciplines and, occasionally, from empirical research conducted by the researcher or others.[98]

In this way, it is possible to identify the 'method' of the socio-logical researcher; utilising the doctrinal scholar's primary legal source materials to identify 'the law in books' but then identifying the necessary 'extrinsic' materials and analysing these to critically evaluate the 'law in action'. In the context of this thesis, the necessary extrinsic materials are likely to be numerous; reports by the Home Office, the Ministry of Justice, the Information Commissioner's Officer and particularly the police themselves are all expected to play a substantial and integral role in identifying the 'law in action' so far as the second, third and fourth research questions are concerned.

Moreover, the recognition that this area of research is as firmly embedded within the sphere of 'criminal justice' as much as it is within 'law' makes a cross-over with the social-sciences almost inevitable, particularly with Criminology. This thesis invokes significant elements of academic criminological research and various criminological concepts and analyses are evident throughout,[99] though perhaps the most notable example is at chapter 8.4, where criminological concepts such as desistence play a central role in an analysis of the continuing need to retain criminality data for operational purposes.

The overlap in this research with the doctrinal approach is self-evident. This thesis will necessarily invoke doctrinal methods in aiming to identify the 'law in books'; this will be made evident throughout the research.[100] There is a growing recognition of the synergy between doctrinal and socio-legal methods[101] and indeed, it has been suggested that,

[97] Above n.85
[98] Ibid
[99] Much of chapter 4, for example, deals with reported offences, police investigative and preventative practices, disposal techniques – subjects which fall very much within the remit of the criminologist.
[100] See, for example, ch.5.3, ch.6.2 and almost the entirety of ch.7.
[101] See, for example, R. Postner, 'The Decline of Law as an Autonomous Discipline: 1962 – 1987' (1987) 100 Harvard Law Review 761

properly synergised, socio-legal research can be utilised to improve doctrine.[102] It is the recognition of this that shapes this research in its attempts to answer the second, third and fourth research questions and, moreover, in the recommendations which are made[103] to amend both law and practice in response to the research findings.

The generation of, and reliance on, empirical data is often considered one of the common elements which differentiates socio-legal research from doctrinal. While not entirely accurate,[104] this thesis will nonetheless attempt to utilise empirical data in support of the theories and critical evaluations made, where this is appropriate. One of the principle criticisms which has been levelled at socio-legal research generally is that lawyers engaged in it often do not have the necessary methodological training required to conduct good quality quantitative data.[105] In recognition of this weakness, this research will instead secondary analysis of primary data collated and published by others.

This is a form of quantitative analysis familiar to the social scientist known simply as 'secondary quantitative analysis'. This method, engaged particularly in chapter 8.4, involves the quantitative reproduction of secondary data reported in other sources. Secondary quantitative analysis of this type effectively 'uses 'old' data for new ideas'[106] and is a useful form of research for the type undertaken here in that there is considerable time and cost savings in not having to undertake the primary data collection.[107]

The first type of data to be utilised in this research is that produced by peer-reviewed publications. The mechanism of peer-review should ensure that the data is of 'good' quality'. The second type of data to be utilised is that produced by the Government in official statistics. This data is a staple of legal, criminological and criminal justice studies[108] and, despite the limitations inherent in these,[109] it is submitted that these represent a realistic' metric by which certain assessments can be made; for example,

[102] Above n.63, 114
[103] See chapter ten of this research
[104] Above n.65, 128 – 132
[105] Above n.76, 44 – 45 and also see L. Epstein and G. King, 'Empirical Research and the Goals of Legal Scholarship: The Rules of Inference' (2002) 69 University of Chicago Law Review 1
[106] Above n.66, 62
[107] Ibid 63
[108] V. Jupp, *Methods of Criminological Research* (Routledge 1999) 47
[109] Ibid, 85 – 127

police ‘clear-up’ rates, if they can be measured at all, can at present only be realistically so done by reference the data produced by the police and the Ministry of Justice who are responsible for these.

The purpose of employing this empirical method is to attempt to identify the ‘law in action’; to ‘fill in the gap’, and to provide support for theoretical positions offered, particularly in attempting to answer the fourth research question.

1.5.3 The Scotland ‘comparison’

At chapter 8.4.2 of this thesis, the research will provide a critical, evaluative commentary of the processes *in situ* for the collation, retention and deletion of criminal records in Scotland.

This might, at first glance, appear to introduce a comparative methodology into this thesis. The term ‘comparative law’ is in itself difficult to define[110] but legal comparative research is broadly thought, at it’s simplest, to involve finding out what the law in a particular country is, and making comparisons to that in another country.[111] The purpose of that comparison is usually intended to be that ‘the national legal system of the observer will benefit by offering suggestions for future development, providing warnings of possible difficulties, giving an opportunity to stand back from one’s own national system and look at it more critically’.[112]

There is a growing trend towards comparative legal research, despite there being no standard method either for selective the comparator or for conducting the comparative research, [113] because the aim of identifying possible ‘solutions’ or legal amendments is considered a ‘valid’ reason for conducting comparative legal research.[114]

However, it is not intended to conduct a ‘comparative’ study with the position in Scotland, in the ordinarily prescribed meaning of the term. This is because direct comparison between differing jurisdictional approaches to the collation and retention of

[110] G. Samuel, *An introduction to Comparative Law Theory and Method* (Hart Publishing, 2014) 8
[111] J. Gourdley, ‘Comparative Legal Research: its function in the development of harmonized law’ (1995) 43 American Journal of Comparative Law 555
[112] Above n.65, 163
[113] K. Zweigert and H. Kötz, *An introduction to Comparative Law* (Oxford University Press 1998) 33
[114] Above n.63, 46

criminal records is fraught with difficulty and (arguably at least) not particularly instructive.

In the United States of America, for example, there is no federal legislation for the central collation of criminality data. Instead, this is collated and stored variously by local police forces, state databases and federal repositories and the data consists predominantly of arrests and 'encounters' with police, rather than court convictions.[115] Moreover, there is no data protection legislation in the United States of America to which criminal record data might be attached).

In Australia, meanwhile, there is a central organisation responsible for the dissemination of criminal records ('CrimTrac')[116] but the data itself is not centralised and is instead held by the individual police forces in each state[117] and is collated and retained in accordance with the polices or legislation applicable to each state.[118] Again, there is no 'national charter of rights' which bears comparison to the ECoHR and criminal record data is considered 'public' data in Australia,[119] which lends it no protection from any data protection legislation.

A brief comparison between England and Wales and EU member states was conducted by the UK government's Independent Reviewer for Criminality Information in 2009. Even this review, which largely consisted of comparison between countries bound by similar privacy and data protection legislation, illustrated the especial difficulties in comparative analysis on criminal record data processes. Some of the more enunciated of these were that different jurisdictions have different means of disposing with criminal matters, particularly in respect of out of court-disposals (such as cautions) and some jurisdictions differentiate in their treatment of juvenile offenders, while others do not. Some criminal record collections are maintained by the police, some by 'criminal record offices', some by a specified government department and others still by the prosecuting authority of that country. Several countries have detailed statutory provisions outlining

[115] J. Selbin *et al*, 'Unmarked: Criminal Record Clearing and Employment Outcomes' (2018) 108(1) Journal of Criminal Law and Criminology 5
[116] B. Naylor, M. Paterson and M. Pittard, 'In the shadow of a Criminal Record: Proposing a Just model of criminal record employment checks' (2008) 32(1) Melbourne University Law Review 171
[117] B. Naylor, 'Criminal Records and Rehabilitation in Australia' (2011) 3(1) European Journal of Probation 79, 82
[118] Ibid, 84 – 86
[119] Ibid, 83

the mechanisms for collating, storing and retaining criminal record data, while others have no statutory mechanisms at all. Some countries do not even store the data on computerised systems.[120]

All of this is intended to illustrate the rather peculiar difficulties in attempting a comparative study as regards the collation, storage and retention of criminal record data between differing jurisdictions. Countries which might ordinarily be considered 'sound' comparators are, for differing reasons, arguably not so in the context of this research. The reality is that there is no consistency of approach which can be identified by states with criminal record collections; whether that be in how the collections are 'governed', what is collected, how it is stored, who stores it and for how long.[121]

This is largely because each jurisdiction has different and competing social, economic, political and industrial concerns which underpin the system they have implemented; American jurists, for example, find themselves wrestling with the issue of free public access to criminal records, afforded to citizens in the wake of the 11 September 2001 terrorist attacks, and the disadvantage suffered by black and other ethnic minority groups who have (disproportionately) received criminal records,[122] rather than any concerns regarding either privacy or data protection.

The rather inevitable result of this is that a comparative analysis is not suitable for research of the type proposed by this thesis. The analysis of the position in Scotland does not intend to represent a 'comparative' analysis in the meaning ordinarily ascribed to it as a legal research methodology, because it is not intended to make recommendations for either legislative amendment or enactment based upon the analysis of the system because it is not possible for this author to state with any authority that the system *in situ* there is 'better' (or, indeed, any 'worse'). Instead, that analysis is offered in order to illustrate an important point; namely that the position in England and Wales is not the only position that could be taken without prejudicing the expressed purposes for criminal record data collation, storage and retention outlined and analysed in chapter four.

[120] S. Mason, 'A Balanced Approach' (Home Office, 2010) Annex D
[121] Ibid, 11 – 12
[122] Above n.85, 9 – 10

An analysis of the criminal record collation and retention system in Scotland, is, it is submitted, instructive and indicative for a number of reasons which would not apply to an alternative jurisdiction and which are oft alluded to by comparative legal researchers. These are as follows:

i. Although Scots Law utilises a different criminal prosecution system than that in England and Wales, there are broad similarities which make a comparison less onerous than other jurisdictions. Criminal cases operate on a two-tier system, where the demarcation line is between 'serious' and 'minor' offences.[123] Decision on bail are impacted by the previous antecedent history of the accused, and these are a statutory factor to be considered in any bail application.[124] Previous convictions and other antecedent matters are admissible as 'bad character' evidence in criminal trials, albeit in more limited circumstances than in England and Wales.[125]

   Criminal conviction details are also a relevant factor in determining sentencing of the defendant after conviction,[126] and a range of broadly comparable court and out-of-court disposals are available under Scots Law, including the provision of fines,[127] community sentences,[128] custody,[129] 'Recorded Police Warnings' (which are broadly comparable to cautions in England and Wales) and 'Anti-Social Fixed Penalties' (broadly comparable to PNfD in England and Wales).[130]

ii. In spite of Scotland having a separate legal system to England and Wales, it shares much primary domestic legislation, including key legislative provisions

[123] In Scotland, 'serious' offences are tried under a 'solemn' procedure, whilst 'minor' offences are dealt with 'summarily'; see Pt. VII and Pt. IX of the Criminal Procedure (Scotland) Act 1995
[124] Per s.23C(2)(d) of the Criminal Procedure (Scotland) Act 1995, as inserted by s.1 of the Criminal Proceedings etc. (Reform) (Scotland) Act 2007
[125] For an extensive evaluation of these, and the current proposals to introduce more extensive provisions in line with those in England and Wales, see F. Stark, 'Wiping the slate clean: reforming Scots Law's approach to evidence of the accused's bad character' (2013) 76(2) Modern Law Review 346 and also Scottish Law Commission, *Report on Similar Fact Evidence and the Moorov Doctrine* (Scot Law. Comm 229, 2012)
[126] See s.101(7) and s.166(7) of the Criminal Procedure (Scotland) Act 1995
[127] Per s.211 of the Criminal Procedure (Scotland) Act 1995
[128] Ibid, s.227A
[129] Ibid, s.204
[130] For an explanation of the use of these out of court disposals, see Scottish Government, 'Criminal Proceedings in Scotland 2017 – 18' (National Statistics, 2018) 40

relating to criminal records (and this research) such as the Data Protection Act 1984, the Data Protection Act 1998, the Data Protection Act 2018 and Police Act 1997 and the Rehabilitation of Offenders Act 1974.[131] This means that the police in Scotland and those in England must largely operate within the same legislative framework; indeed, 'Data Protection' is a 'reserved matter' for which the devolved Scottish Parliament has no power to legislate and is instead bound by legislation from Westminster.[132]

iii. The system of criminal record collation and retention in Scotland has run almost parallel to that in England and Wales. Although outlined in depth at chapter 2 of this research, some indicative examples of this include the statutory imposition of a police obligation to initiate a 'criminal record register' in Edinburgh under the provision of the Prevention of Crimes Act 1871,[133] the creation and operation (within a decade or so) of police 'criminal record offices' modelled on that opened at Scotland Yard[134] and the opening of a 'Scottish Criminal Record Office' in Glasgow during the period of decentralisation in the 1960s.[135] The SCRO computerised it's records in 1988[136] and the current system, the Criminal History System ('CHS'), performs a 'similar service' to the PNC in England and Wales.[137]

iv. Policies for data collation, storage and disclosure have also run almost parallel, with the major changes initially stemming from circular documents,[138] followed by Part V of the Police Act 1997 and the creation of 'Disclosure Scotland'; a public-private partnership which almost exactly mirrors the CRB/DBS in England and Wales.[139] As is the case in England and Wales, the policies which govern the collation, storage and retention of criminal records data on CHS are not

[131] Albeit that legislative changes are now well advanced to introduce a less restrictive version of the Rehabilitation of Offenders Act 1974 by the introduction of the Management of Offenders (Scotland) Bill 2019
[132] Per the Scotland Act 1998, Sch.2, Pt.2(3)(B2)
[133] Per s.6(3) of the Prevention of Crimes Act 1871
[134] Above n.35, 18
[135] A.G. Ralston, *The Real Taggarts: Glasgow's Post-War Crimebusters* (Black and White Publishing 2017)
[136] D. Leask, 'Police investigate tough drugs policy' *The Herald* (Glasgow, 8 April 2008)
[137] Her Majesty's Inspectorate of Constabulary, 'Scottish Criminal Record Office. Primary Inspection 2004' (2005) para.5.112
[138] Scottish Office (Police) Circular No.4 of 1989
[139] Above n.99, para.5.32

prescribed by statute but are instead delegated to the police; formerly instigated by the Scottish equivalent to ACPO ('ACPO Scotland') and now Police Scotland.[140]

v. Such is the interrelationship between Scottish police and their English counterparts that police in England and Wales routinely co-operate with their Scottish counterparts in criminal records and related criminality data matters. Scottish police have access to the PNC, including the PHOENIX database, and are able to create and amend records, including the routine uploading of CHS data onto the PNC.[141] A similar data sharing arrangement is in place for the PND; Scottish forces have access to the PND and information from the Scottish equivalent ('The Scottish Intelligence Database') and CHS are uploaded onto the PND for use by English and Welsh police forces.[142]

It is for these reasons that an instructive analysis of the system for criminal record data collation, storage and retention in Scotland is pertinent to a doctrinal analysis of the system in England and Wales. It is not a 'comparative analysis' as it is not intended to show that one system is 'better' than another; in fact, the purpose of this analysis is to illustrate by way of comparable example that there is an extant alternative system of retention *in situ*, even where the justifications for retention are broadly the same as those offered by the NPCC.

1.6 Conclusions

In order to test the hypothesis that the traditional view that 'criminal records' are centrally held records of court convictions, this research will utilise a doctrinal approach to ascertain what records have been collected, what records continue to be collected and whether these merit a reconsideration of the traditional definition.

In order to test the hypothesis that the police are likely to have committed breaches of the DPA 1984 and the DPA 1998, this research will use a doctrinal approach to identify

[140] Formed after the Scottish Government legislated to merge all eight Scottish police forces into one single force on 1 April 2013; see s.6 of the Police and Fire Reform (Scotland) Act 2012
[141] Above n.99
[142] Justice Sub-Committee on Policing, 'Police Scotland's Digital Data and IT Strategy: Evidence Session' (Scottish Parliament, 10 May 2018) Written Submission, Police Scotland

whether there is evidence to suggest that this has taken place, when, how and, if possible, why.

In order to test the hypothesis that the police policy regarding the length of time that records are retained is ‘excessive’, the research will invoke a mixture of doctrinal, comparative and quantitative methods to identify legal, social and economic rationale for questioning the *status quo*. The research will conclude by making conclusions and recommendations based on these findings.

2

The historical development of a national collection of criminal records in England and Wales

2.1 Introduction

Criminal data collection is not a new phenomenon in England and Wales. The general public perception that criminal activity is socially disruptive and there is, therefore, a public interest in recording information relating to the individuals involved, has existed since at least the mid-eighteenth century in England and Wales.[1]

This chapter aims to provide an abridged, critical chronology of the development of a national collection of criminal records in England and Wales. In doing so, it is intended to identify the principal staging points in the building of the modern criminal record collection, identifying the early origins of data retention, and critically evaluating who collected data, what was being collected and why collections were undertaken at all. The identification of these elements is intended to assist in framing the analysis of the modern collection, both as comparators and also as a means of asking whether lessons might be learned and, if so, whether they have.

2.2 1730 – 1869: the embryonic collections

The first formal criminal record collection involved the institution of a public office at Bow Street in 1739, where a justice was available to record reports of crimes.[2] In 1748, Henry Fielding was appointed as Chief Magistrate at Bow Street.[3] He then appointed a register clerk to take details of crimes reported, stolen items and the names of those suspected and/or convicted of offences.[4] John Fielding succeeded his half-brother and in 1754 he opened a rudimentary 'criminal records office'[5] to collect allegations of criminality, notes

[1] N. Mustafa et al, 'An exploration of the historical background of criminal record checking in the United Kingdom: from the eighteenth to the twenty-first century' (2013) 19 European Journal of Criminal Policy and Research 15
[2] R. Shoemaker, *The London Mob: Violence and Disorder in Eighteenth-Century England* (Cambridge University Press 2004) 40
[3] Above n.1,16
[4] T. Thomas, *Criminal Records, A Database for the Criminal Justice System and Beyond* (Palgrave Macmillan 2007) 106.
[5] S.Tong et al, *Understanding Criminal Investigation* (Wiley-Blackwell 2009) 3

of warrants issued, convictions and sentences.[6] This data was disseminated routinely to local policing groups and magistrates, expressly to assist in the apprehension of wanted criminals.[7] This was done by publication in 1771 of the *Quarterly Pursuit* and the *Weekly or Extraordinary Pursuit*,[8] which in 1786 became the *Hue and Cry*.[9] Criminality data continued to be retained at Bow Street until 1780, when the entire collection was destroyed (perhaps deliberately[10]) in the Gordon Riots.[11]

Shoemaker and Ward have argued that these early collections were motivated by 'a broad moral and empirically driven desire to better understand the criminal and the causes of crime.'[12] It is submitted, however, that it is unlikely that these rudimentary collections were instituted through mere criminological curiosity. In truth, Henry Fielding came to Bow Street 'during a crime wave'.[13] He had three conjoined objectives: 'to establish a systematic criminal intelligence and information gathering apparatus; to create a coherent police administration centre and to develop a preventative strategy for crime management'.[14] John Fielding created the 'Bow Street Runners' – a collection of paid thief-takers which formed the basis of what many consider the first rudimentary police force[15] – in the hope of achieving his brother's second and third aims. His criminal record collection was instituted, it is submitted, to meet the first.

The Fielding brothers didn't simply use their criminal record collection for philanthropic purposes. They also used them to make money. The original Bow Street list formed the basis of Henry Fielding's 'Universal Register Office' – a rudimentary employment agency

[6] J. M Beatie, *The First English Detectives: The Bow Street Runners and the Policing of London, 1750 – 1840* (Oxford University Press 2012) 28
[7] T. Weller, I*nformation History in the Modern World: Histories of the Information Age* (Palgrave MacMillan 2011) 17
[8] Ibid
[9] G.J. Dunston, *Whores and Highwaymen: Crime and Justice in the Eighteenth-Century Metropolis* (Waterside Press 2012) 328 – 9
[10] According to Thomas, the records were 'carefully selected' by the supposedly unruly mob: see T. Thomas, *The Registration and Monitoring of Sex Offenders: A Comparative Study* (Routledge 2011) 14.
[11] Above n.6, 12
[12] R. Shoemaker & R. Ward, 'Understanding the criminal: record-keeping, statistics and the early history of Criminology in England' (1 November 2017), 57 The British Journal of Criminology 6 1442, 1444
[13] M. Palmiotto & N. Prahba Unnithan, *Policing and Society, A Global Approach* (Delmar Cengage Publishing 2011) 166
[14] J. McMullan, 'Policing reform and moral discourse: the genesis of a modern institution' (1998) 21 (1) Policing: An International Journal of Police Strategies and Management 137, 139
[15] P. Collins, T.A. Ricks & W. van Meter, *Principles of Security and Crime Prevention* (Routledge London 2015) 14.

which opened in London in 1749.[16] Fielding used his collection here for the purpose of employment vetting, pronouncing that, in return for sixpence paid: 'no servant shall ever be registered who cannot produce a real good character from the last place where he or she actually lived'.[17] The desire of both Henry and John Fielding's to generate profit from policing criminality was widely recognised: McMullan latterly described the Bow Street Runners as 'monied police encouraged to engage in civil mercenary work, taking their profits from state rewards, fees and private enterprises'.[18]

From around 1780, criminality information was being collated locally 'without compulsion from the central state',[19] particularly at prisons, where staff were especially active in collecting information on their inmates.[20] The Home Office was instituted in 1782, but as 'crime was not a high priority for Home Office officials', it initially took little interest in criminality information.[21] This was hardly surprising: Parliament was responding to the 'crime wave' by simply increasing the number of capital offences. The so-called 'bloody code', intended to prevent offending by deterrent, [22] meant that by 1815, the number of capital offences on the statute book stood at around 225.[23] The principal alternative was transportation. Although in some limited use previously,[24] transportation was formally incorporated onto the statute books in 1718 in the hope that it would both remove criminals from society and solve a labour shortage in the colonies, particularly in North America.[25] The American Revolution ended the practice there and instead convicts were sent to New South Wales.[26]

Where an offender faced a death sentence or permanent transportation, there is little purpose in retaining criminality data regarding him, save for statistical purposes. Deceased offenders do not commit further offences, and while those banished from the country may reoffend, they do so elsewhere and thus outside the scope (and concern) of

[16] M. Bichard, 'The Bichard Inquiry Report' (HC 653, 22 June 2004) 56
[17] H. Gladfelder, *Criminality and Narrative in Eighteenth-Century England: Beyond the Law* (John Hopkins University Press 2001) Part III
[18] Above n.14, 140
[19] Above n.12, 1443
[20] Ibid
[21] Ibid,1445
[22] F. McLynn, *Crime and Punishment in Eighteenth Century England* (Routledge 1989) 257
[23] Ibid, xi
[24] H. Johnston, Crime in England 1815 – 1880: Experiencing the Criminal Justice System (Routledge 2015) 73
[25] Part I of the Transportation Act 1718
[26] Above n.22

the government. The retention of information relating to those offenders would, therefore, have been unduly cost-prohibitive for the newly formed, and funding deficient, Home Office. However, transportation was not ordinarily intended to be permanent; indeed, periods of 'seven years minimum' were usually thought to provide the desired deterrent effect.[27] It is perhaps understandable, therefore, that the Home Office was prepared to take control of a rudimentary collection of criminal conviction data started by the City of London in 1791[28] when it became too expensive for the City to maintain it in 1793.[29] This marked the first time that a criminal record collection lay in the hands of the government in England and Wales.

In 1800, transported convicts in New South Wales were being offered an embryonic form of parole known as a 'ticket-of-leave'. This allowed the convict to obtain work prior to the conclusion of their sentence, under supervision and on the condition that the 'ticket' would be revoked if a new offence was committed.[30] The ticket itself contained 'identifying information about the convict and characteristics and details of their criminal history'.[31] This allowed the Home Office to put its newly obtained collection of criminality information to some use, sharing data with prison administrators and local magistrates in Australia. Although transportation became unpopular and pressure mounted to abandon it,[32] the ticket-of-leave' system was considered a success.[33] The Penal Servitude Act 1853 ended transportation in all but exceptional cases[34] and made two fundamental changes to domestic law: it introduced imprisonment as the predominant alternative means of punishment[35] and brought the 'ticket of leave' system to England and Wales.[36]

This resulted in criminality information being used by the state in England and Wales for the first time in the administration of justice, with convictions data being used to inform the decision of the Office of the Director of Convict Prisons on whether a ticket should be

[27] Above n.24, 74
[28] Above n.12, 1446
[29] Many of these have been preserved by the National Archives: see Metropolitan Police: Criminal Records Office: Habitual Criminal Registers and Miscellaneous Papers (MEPO 6, 1834 – 1959)
[30] S. O'Toole, *The History of Australian Corrections* (UNSW Press 2006) 125
[31] Above n.22
[32] Above n.22, 290 – 91
[33] T. Thomas, *The Registration and Monitoring of Sex Offenders: A Comparative Study* (Routledge 2011) 16
[34] Per s.1 of the Penal Servitude Act 1853
[35] Per s.2 of the Penal Servitude Act 1853
[36] Per s.9 of the Penal Servitude Act 1853

issued.[37] However, the system ran into almost immediate problems. Criminologists familiar with modern media crime reporting would recognise the contemporary lamentations that convicts with tickets re-offended[38] or that the system was excessively lenient, which turned public opinion against the system and generated a widespread fear of the 'habitual criminal'.[39] Men with tickets therefore found it difficult to find work,[40] which in turn encouraged them to lie about their identities[41] or, ultimately, to return to criminality.[42]

Sir Walter Crofton, responsible for implementing a similar system in Ireland, lamented that the system was failing in England because 'we entirely neglected to adopt the colonial safeguards, viz, the supervision of the liberated convict and his re-confinement to prison in the event of misconduct'.[43] When the Home Office tasked the Commissioner of the Metropolitan Police to provide a report on the ticket-or-leave men, they were told that the police 'could not find or produce a single man of them'.[44] When the police did eventually find one, officers were accused of revealing their identifies to employers and often became overzealous in returning them to custody.[45] Despite reforms introduced by the Penal Servitude Act 1864, the system was considered by 1869 'an absolute failure.'[46]

2.3 1869 – 1910: national statutory and police criminality data collation

The failure to properly supervise ticket-of-leave men meant that 'the Victorians…wanted a national system of registering known criminals.'[47] The result was the Habitual Criminals Act 1869 ('the HCA 1869')[48] which is 'now taken as the starting point for the statutory

[37] P.J. Murray, 'Not so bad as they seem: The Transportation, ticket-of-leave, and penal servitude questions, plainly stated, and argued on facts and figures, with come observations on the principles of prevention, in a letter addressed to Matthew Devenport Hill' (1857) Knowsley Pamphlet Collection 13 – 14
[38] Above n.33, 17
[39] T. Thomas, *Sex Crime, Sex Offending and Society* (Routledge 2015) 42
[40] W. I. Aislabie, *The Ticket-of-Leave System in Australia and England Volume 1* (Effingham Wilson, London 1857) 4
[41] Ibid, 7 – 8
[42] Ibid, 5
[43] W. Crofton, 'Convict systems and transportation: a lecture delivered at the Philosophical Institution, Bristol, on the 22nd December 1862' (LSE Selected Pamphlets 1963) 3
[44] L. Radzinowicz and R. Hood, *The Emergence of Penal Policy in Victorian and Edwardian England* (Clarendon 1990) 249 cited in T. Thomas, Sex Crime: Sex Offending and Society (Routledge 2015) 42
[45] Above n.33, 18
[46] Above n.39, 43
[47] Above n.38, 19
[48] T. Thomas, 'National collection of criminal records – a question of data quality' (November 2001) Criminal Law Review 886, 886 – 887

collation of the United Kingdom's repository of criminal records'.[49] Section 5 of the HCA 1869 provided that 'a register of all persons convicted of a crime shall be kept' and that responsibility for the list lay with the police in London and Dublin. An 'Alphabetical Register of Habitual Criminals' was duly created, maintained at Scotland Yard[50] by the Commissioner of Police of the Metropolis, who became known as 'the Keeper of the Records'[51] and published routinely in bound volumes.[52] The intention behind the register was clear: one MP declared it to be nothing less than: 'a wholesale system of police surveillance, so that a considerable portion of the people would be in a state of out-of-door imprisonment, tied, as it were, by the leg to the police'.[53]

The scope of the proposed scheme was enormous and, in fact, 'the number of persons registered accumulated so rapidly…that the register was almost useless from its bulk'.[54] Other problems quickly manifested. Those wishing to consult the register had to travel to London or Dublin to do so,[55] limiting its usefulness in the provinces. The register omitted any offences/offenders in Scotland, as the HCA 1869 made no provision for their inclusion.[56] There were no provisions made for the identification of offenders; the reigster was simply a list of names and convictions, with little to match records to individuals save sporadic photographs provided by prison staff.[57] This meant that 'a convict could evade official knowledge of his prior convictions simply by giving a false name'.[58]

Parliament attempted to rectify these problems by implementing the Prevention of Crimes Act 1871, which repealed the 1869 Act[59] and introduced more wide-ranging provisions. New registers were to be established in London,[60] Edinburgh,[61] and Dublin[62] and only those convicted twice or more were included in it.[63] Conviction details and photographs

[49] Above n.4,11
[50] R. Williams and P. Johnson, *Genetic Policing: the uses of DNA in police investigations* (Willian Publishing 2008) 21
[51] Ibid, 21 – 22
[52] Above n.50
[53] HC Deb 4 August 1869, Col. 1261, cited in T. Thomas, *Sex Crime, Sex Offending and Society* (Routledge 2015) 44
[54] E. F. Du Cane, *The Punishment and Prevention of Crime* (Read Books 2013) ch.7.1
[55] Ibid
[56] Above n.49
[57] Above n.47
[58] S. Cole, *Suspect identities: a history of fingerprinting and criminal identification* (Harvard University Press 2001) 19
[59] Per s.21(1) of the Prevention of Crimes Act 1871
[60] Per s.6(2) of the Prevention of Crimes Act 1871
[61] Per s.6(3) of the Prevention of Crimes Act 1871
[62] Per s.6(4) of the Prevention of Crimes Act 1871
[63] Per ss.7 – 8 of the Prevention of Crimes Act 1871

were to be provided by prison governors on a prescribed form. [64] Governors who did not comply risked a fine of up to twenty pounds.[65] Arrangements were made for convict prisoners to print the records as they were updated, and the prints were circulated to police forces and prisons nationwide.[66] The first volume contained 12,164 names with 21,194 convictions listed against them.[67]

The identification problem persisted[68] and a 'Register of Distinctive Marks' – 'an ambitious if cumbersome attempt to describe systematically the vagaries of the human body' – was instituted in an attempt solve it.[69] The intention was to provide the police with 'all information necessary to establish a *prima* facie identification of any person suspected of being an habitual criminal…These two books give the particulars necessary to assist the police in their attempts to check the habitual criminal in his career'.[70] The reality, however, was that the sheer volume of data collected continued to cause problems because many of those listed 'were not habitual criminals in the ordinary sense'.[71] Searches sometimes resulted in 'false-positives', so that the wrong record was attached to the wrong person, leading to them being incorrectly labelled a repeat offender.[72] The production of annual bound volumes, rather than in card index as propounded by jurist Arnould Bonneville de Marsangy some thirty years previously, [73] meant that records were often out of date as quickly as they were published; a particular problem for a system which relied on given names, convict descriptions, bodily markings and photographs, which is many cases might change quite markedly over even a single year.[74]

Moreover, the entire process was extraordinarily laborious. By 1875, the London Alphabetical Register contained some 150,000 names and some 30,463 photographs. Manual searching of this vast repository took a very long time and yielded comparatively few results: in 1872, for example, the police obtained just 373 positive identifications.[75]

[64] Above n.58, 20
[65] Per s.6(5) of the Prevention of Crimes Act 1871
[66] Above n.54, ch.7, 2
[67] Ibid
[68] Above n.58, 26
[69] Ibid
[70] Above n.66
[71] Above n.58, 27
[72] Above n.58, 28
[73] Ibid, 28 – 29
[74] Above n.71
[75] B. Godfrey, D. Cox and S. Farrall, *Serious Offenders: a study of habitual criminals* (Oxford University Press 2010) 97 – 8

Even an abridged register, created in 1877 to try to mitigate the problems of scale and labour, did not significantly improve matters; indeed, the police barely used it[76] and 'the knowledge in the heads of policemen on the beat' was still the principal means utilised to detect crimes and apprehend suspected offenders.[77]

Against this backdrop, a 1874 Home Office report declared the entire system 'a comparative failure'[78] but did not recommend that it be halted. Rather, in 1877, the task of maintaining the Alphabetical Register was transferred to the Prisons Department of the Home Office,[79] who opened a Habitual Criminals Registry ('the HCR') for that purpose.[80] Meanwhile, the police constabularies in Liverpool and Birmingham, still bedevilled by the inherent difficulty in obtaining information from the Alphabetical Register and under a statutory duty to supervise convicts, began to keep their own collections.[81] These registers, however, were not intended to be as comprehensive as that kept at the HCR, and the force in Liverpool, for example, still used the national register when searching for a suspect on the basis of description evidence.[82]

The Metropolitan Police, also struggling to fulfil their supervisory obligations and no longer in possession of the Alphabetical Register,[83] attempted to rectify their problems by establishing a Convict Supervision Office at Scotland Yard ('the CSO').[84] The CSO collated their own criminality data separate from, though often confused with, that of the HCA.[85] This was deemed necessary to facilitate the work of the CSO, which included visiting convicts at prison prior to release, helping to obtain employment[86] and verifying residency post-release[87] and was, therefore, essentially 'probationary' in nature[88] The

[76] E. Higgs, *Identifying the English: A History of Personal Identification 1500 to the present* (Continuum Publishing 2011) 95
[77] Ibid at 96
[78] Above n.38, 20
[79] J. F. Moylan, *Scotland Yard and the Metropolitan Police* (G.P Putnam & Son 1929) 190
[80] W. L Melville Lee, *A history of police in England* (Methuen & Co 1901) 359
[81] Above n.76, 96
[82] Ibid.
[83] Above n.39, 44
[84] H. Shpayer-Makov, *The ascent of the detective: police sleuths in Victorian and Edwardian England* (Oxford University Press 2011) 49
[85] Above n.76, 96
[86] Above n.75, 98
[87] Above n.85
[88] G. Mair and L. Burke, *Redemption, Rehabilitation and Risk Management: A History of Probation* (Routledge 2012) 22

CSO also kept their own registers of distinctive marks, convict descriptions[89] and a photograph collection.[90]

The CSO collection reflected the Metropolitan Police's belief that, despite the comparative failures of the statutory registration schemes, the majority of crimes were committed by 'habitual' criminals and such individuals should therefore be monitored.[91] The CSO's primary criminal record function was, therefore, surveillance; during the first six years of its operation, the CSO claimed it had 'kept track of most habitual offenders and convicts released on licence'[92] and officers claimed that the register's capacity to allow the police to monitor such men was 'of inestimable value in the prevention of crime'.[93]

The data was not just used for crime prevention, however. The CSO record collection has been described as 'the first systematic attempt to create a centralised source of police information for the purposes of suppressing deviancy'.[94] The perceived value of criminality data in detective work began to emerge, with police officers investigating new offences matching witness accounts and details found at crime scenes with descriptions and pictures held in the CSO registers.[95] Building on these principles, in 1883 the CSO used their records to print and disseminate to all forces the *Police Gazette*; *a successor to Hue and Cry*[96] which provided confidential 'intelligence' relating to 'people wanted, new crimes committed and offenders being discharged from prison'.[97]

The use of criminality data for the detection, rather than the prevention, of crime was perceived to be relatively novel in the nineteenth century but it was, in truth, little more than a more large-scale re-application of the principles first espoused by the Fielding brothers at Bow Street a century before. However, this model of utilising criminality data as 'intelligence' to inform detective work – a rudimentary form of what a century later would become known as 'intelligence-led policing'[98] – was mimicked by several provincial

[89] Above n.75, 97
[90] B. J. Rahn, *The Real World of Sherlock* (Amberley Publishing 2014) Ch.5, 3
[91] R. B. Fosdick, *European Police Systems* (The Century Co 1915) 316
[92] M. J. Wiener, *Reconstructing the Criminal: Culture, Law and Policy in England, 1830 – 1914* (Cambridge University Press 1990) 265
[93] G. Dilnot, *Scotland Yard: the methods and organisation of the Metropolitan Police* (Marschall London 1915) 58
[94] C. McCartney, *Forensic Identification and Criminal Justice* (Routledge 2012) 106
[95] Above n.80, 360
[96] Above n.9
[97] Above n.4,13
[98] J. Ratcliffe, *Intelligence–Led Policing* (Routledge 2016) 4

forces[99] and was credited with what many Victorians referred to as 'the English miracle of falling crime rates'.[100]

The reality, however, was that this perception was a mirage. A Departmental Committee established to investigate the official crime data found it 'next to useless'.[101] Moreover, the reality of the CSO's supervision programme was found to be rather different than that painted by the CSO themselves: in reality they were 'haphazard and unbureaucratic'[102] – in 1888, the CSO assigned twelve staff to supervise some 32,000 convicts.[103] Underfunded and understaffed, police forces were incapable of effecting proper supervision[104] and the same problems of absconding,[105] lack of public support[106] and over-zealous policing[107] which undermined the ticket-of-leave programme began to infect convict supervision so that the perceived reality which emerged was that 'if a man is determined to do wrong all the supervision in England will not prevent it. The police cannot always watch a man'.[108]

The revelation that supervision was not preventing crime did little to discourage the police from collecting criminality data. Encouraged by the apparent usefulness of the data in detective work, both CSO and the Habitual Criminals Registry continued to collect data with a renewed focus on building repositories of information useful to Criminal Investigation Departments (CID). Guided by little more than a desire to collect as much information as possible, the CSO did not learn from the mistakes of the first habitual criminals register and their collection became so unwieldy that the time and effort required to yield positives results was wholly disproportionate: one parliamentary committee found in 1893 that 21 officers took 57.5 hours to search the register for 27 prisoners and yielded seven identifications.[109]

[99] Above n.80
[100] Above n.75, 69
[101] Ibid, 72
[102] Above n.89
[103] Ibid
[104] Above n.92, 304
[105] H. Johnson, *Crime in England 1815 – 1880: Experiencing the Criminal Justice System* (Routledge 2015) 36
[106] Above n.104
[107] Above n.105, 36
[108] Above n.39, 44
[109] Above n.76, 97

Such problems probably explain why the CSO failed to become the hub of criminal intelligence as it had intended,[110] despite the decision of a Home Office committee to return custody of the Alphabetical Register to Scotland Yard in 1894,[111] consolidating the national collection once more into a single repository in the hands of the Metropolitan Police.

The major problem in trying to accurately identify an individual in and tie him to his criminal history among a collection of hundreds of thousands of records persisted. The CSO initially attempted to resolve this by recording yet more information, including more photographs, initials, distinctive marks (including tattoos) and a classification of the individuals' *modus operandi*.[112] This was then supplemented by the implementation of the *anthropometric system*[113] devised by the head of their counterpart organisation in Paris, Dr. Alphonse Bertillon, in 1882,[114] which involved the physical measurement by calipers and recording of eleven different bony parts of the suspect's body, taken under controlled conditions.[115] Bertillon claimed that his system worked because the odds of two people having the same measurements were 4,191,304 to 1.[116]

This system had a number of limitations; the intricate measurements required meant it was inefficient, it did not reflect natural changes to the body over time or through illness and it was expensive and heavily dependent on the quality of the work undertaken by the technicians involved.[117] The identification problem was evidently unresolved, in spite of a growing acceptance that 'the usefulness of criminal records depends on the ability to fasten upon each human being an identity from which he cannot escape'.[118]

---

[110] Ibid
[111] Home Office, 'Report of a Committee appointed by the Secretary of State to inquire into the best means available for identifying Habitual Criminals' (1893 – 94) LXII
[112] J. Pratt, *Governing the Dangerous: Dangerousness, Law and Social Change* (The Federation Press 1997) 12
[113] N. Morland, *Science against Crime* (Exeter Books 1984) 24
[114] A. Vollmer, 'The Criminal Identification Bureau', (November 1918) 9(3) Journal of the American Institute of Criminal Law and Criminology 322, 323
[115] E. E. Hueske, *Firearms and Fingerprints* (Infobase Publishing 2009) 44
[116] Ibid
[117] R. Craib, *The Cry of the Renegade: Politics and Poetry in Interwar Chile* (Oxford University Press 2016) 125
[118] Above n.91, 319

In 1900, a committee chaired by Henry Belper[119] was convened by the Home Secretary to consider the most appropriate means of attaching criminal records to individuals.[120] The choice was between anthropometry or an alternative system proposed by Sir Edward Henry, the Inspector General of Police for the Bengal Province of India.[121] Henry was not convinced by the anthropometric system and liaised with Sir Francis Galton to produce an alternative.[122] Galton was convinced that the marks on the hand and fingertips were a permanent[123] and unique[124] identity marker and, having unsuccessfully attempted to persuade the government in 1873 to adopt fingerprinting as a means of criminal identification,[125] he turned over all his work to Henry in 1890.[126]

Henry developed a classification for use in Bengal[127] and, by the time the Belper Committee was convening, the 'Henry Classification System' had helped secure its first criminal conviction when a thief was matched by his criminal record to a bloody mark left at a crime scene in Bengal in 1898.[128] An independent review of his system, conducted in 1897 by the British Indian Government, had concluded that fingerprinting was simpler, cheaper, quicker and more reliable than the anthropometric system and so they abandoned the latter in favour of the former.[129] The Belper Committee recommended that England and Wales do likewise.[130] Henry was subsequently made an assistant commissioner of the Metropolitan Police[131] and duly opened a Fingerprint Registry at Scotland Yard on 1 July 1901,[132] with three officers from the anthropometric department at Scotland Yard were tasked with converting their anthropometric criminal record collection into useable fingerprint records.[133] In 1902, one of the officers matched the

[119] Home Office Committee, 'The workings of the methods of identification of criminals by measurements and fingerprints, and the administrative arrangements for carrying the system' (1900)
[120] Above n.58, 91.
[121] Above n.118, 165
[122] F. Galton, *Fingerprints* (MacMillan and Co: London 1892)
[123] Ibid, 1
[124] Ibid, 8
[125] E. Holder, T*he Fingerprint Sourcebook* (National Institute of Justice 2011) 1–13
[126] D. Ashbaugh, *Quantitative–Qualitative Friction Ridge Analysis: an introduction to basic and advanced Ridgeology* (CRC Press 1999) 32.
[127] Ibid, 33
[128] G.S. Sodhi and J. Kaur, 'World's First Conviction on Fingerprint Identification' (2003) National Crime Records Bureau Gazette 15(2), 1–3
[129] Above n.125, 1–14
[130] Ibid at 1–15
[131] I. Pepper, *Crime Scene Investigation: Methods and Procedures* (Oxford University Press 2010) 80.
[132] L. Yount, *Forensic Sciences: From Fibers to Fingerprints* (Chelsea House Publishers 2007) 29
[133] T. Thompson and S. Black, *Forensic Human Identification: An Introduction* (CRC Press 2007) 61

criminal record of Harry Jackson to fingerprints found at the scene of a burglary in London, and subsequently obtained the first conviction in England to rely on fingerprint evidence.[134]

Although the value of fingerprinting as a detective tool was not initially realised – at this stage 'police departments were primarily interested in using fingerprints to index criminal records' and fingerprinting for investigating crimes was 'a mere side-line to the real work of maintaining a criminal record archive[135] – the identification problem was solved. The improvement in efficiency was marked: the number of positive identifications of offenders and their criminal records using the anthropometric system in 1901 was 410; in 1902, the change to fingerprinting yielded 1,722 comparable identifications.[136] Attempts to compile a comprehensive fingerprint register began in earnest and by 1909, the Fingerprint Registry had compiled 140,000 records[137] and fingerprinting remains the pre-eminent means of identifying offenders today.

Around the same time that fingerprinting was solving the identification problem, efforts were finally being made to implanted Bonneville de Marsangy's solution to the problem of publishing bound volumes of records which are out of date almost immediately upon publication.[138] His solution was to 'treat criminal bodies as librarians treat books'[139] and create an index-card system. This system, first trialled for criminal records data by police in Liverpool,[140] allowed for records to be contained in alphabetical ordered files which were simply amended as the need arose, without disrupting the order of the records.[141] A similar system was successfully trialled at the CSO in 1896[142] and then expanded to all of Scotland Yard in 1904.[143]

[134] Ibid. The first recorded use of fingerprints by police to identify a perpetrator in Europe is usually attributed to the slightly earlier success of Bertillon, the inventor and chief proponent of the competing anthropometry system, who used prints on one of the records kept in Paris to secure a conviction on 24 October 1902 (see P. Virilio, *The Vision Machine* (Indiana University Press 1994) 42).
[135] Above n.58, 194
[136] Above n.2
[137] J. Agar, *The Government Machine: A Revolutionary History of the Computer* (The MIT Press 2003) 140
[138] Above n.58, 16
[139] Ibid, 18
[140] C. A. Williams, *Police Control Systems in Britain 1775 – 1975: from Parish Constable to National Computer* (Manchester University Press 2014) 100
[141] Above n.139
[142] Above n.137
[143] Above n.140

The Convict Supervision Office and the Habitual Criminals Registry were formally merged in 1905[144] but this combined registry, whilst vastly improved, still failed to become 'the first port of call' for provincial forces and comparable local facilities were instituted at Wakefield and Hatfield, among others.[145] Scotland Yard responded by revamping the *Police Gazette* in 1910 to improve the sharing of criminal intelligence from Scotland Yard to provincial forces (including new intelligence on 'travelling' and 'expert' criminals).[146] This meant there finally existed something approaching 'a reliable criminal records system'.[147] In 1913, the Habitual Criminals Registry was merged with the Fingerprint Agency, and the Criminal Records Office ('the CRO') was opened at Scotland Yard.[148]

What is clear, therefore, is that, from the kernel of the isolated 18th century initiatives at Bow Street and a smattering of local prisons, the nineteenth century saw an exponential growth of interest in the collation of data relating to offenders and their offences. The state, previously disinclined to so much as count how many offenders were consigned to the gallows and the hulk, suddenly deigned it pertinent to institute two national registers and to collect huge amounts of criminality data, ranging from convictions handed down in court to the caliper measurements of an offender's elbow. The desire to collect, and to ensure collection was accurate, led directly to the development of one of the cornerstones of modern forensic science.[149]

What is not at all clear is what drove this expansionist programme. The author has previously highlighted the proposition that 'criminological curiosity' drove the programme of criminal record collation,[150] while Higgs argues that the criminal record collection was symptomatic of a wider process which saw England becoming an 'information state',[151] with those in charge simply 'devoted to the collection and manipulation of personal data about their subjects'.[152] In essence, this argument provides that the government started collecting data became it could; a collection for collecting's sake. Others have suggested that initiatives to chart criminal behaviour and document those responsible were a form of

[144] Above n.4, 22
[145] Above n.76, 115
[146] Above n.39, 49
[147] A. Moss and K. Skinner, *The Victorian Detective* (Shire Publications 2013) 52
[148] Above n.84, 322
[149] A. Kamilah Muda et al, *Computational Intelligence in Digital Forensics: Forensic Investigation and Applications* (Springer 2014) 55
[150] Above n.12
[151] Above n.76, 10 – 27
[152] Above n.12, 1443

'nation modelling'; an attempt to explain social and economic issues though an 'understanding of national trends'.[153]

It is submitted that, although there are elements of truth in all of these theories, the practical reality is that the data was collated by those involved intrinsically believed that it would somehow help in the prevention of crime. The Fielding brothers thought criminal records would help their rudimentary police force prevent crime. The legislative programmes of the mid-late nineteenth century came about because Parliament were concerned that habitual offenders might commit more crime if released unsupervised back into society. Supervision meant, in effect, crime prevention. Such was the prevalence of the doctrine that criminal records aided in crime detection that Vollmer wrote in 1918 that 'only unimportant cities or cities who inhabitants are lacking in civic pride lack identification bureaus'.[154]

2.5 The Criminal Records Office: the 'crooks clearinghouse'

The amalgamation of the three principal national collections of criminality information into the Criminal Records Office ('the CRO') at Scotland Yard was intended to form 'a national registry of crimes and criminals'.[155] The CRO brought a period of comparative stability to the criminal record process itself – it's mechanisms remained largely unchanged from its inception up to the late 1980s[156] – by embarking upon a criminality data collation and storing exercise which was 'systemised in a manner and to an extent not hitherto attempted'.[157]

What was also clear was that the purpose of the collection had changed. Winston Churchill, upon being appointed as Home Secretary in 1910, declared himself against making specific provisions for supervising habitual offenders, describing the extant legislation as 'unsatisfactory'.[158] While expressing his admiration for the work of police in fulfilling their ticket-of-leave obligations, he told Parliament on 20 July 1910 that the entire 'ticket of leave' system had a 'negative value as regards rehabilitating offenders'.[159] He

[153] J. Innes, *Inferior Politics: Social Problems and Social Policies in Eighteenth Century Britain* (Oxford University Press 2009) 143.
[154] Above n.114, 324
[155] Above n.84, 322
[156] Above n.39, 49
[157] S. Petrow, *Policing Morals: The Metropolitan Police and the Home Office 1870 – 1914* (Clarendon Press 1995) 86
[158] HC Deb 20 July 1910, vol.19, col.352
[159] E. Moritz, *Winston Spencer Churchill and Social Reform* (University of Winconsin 1953) 179

immediately suspended the system and asked for legislation to be brought to abolish it;[160] this speech effectively ended the police supervision of habitual offenders.[161]

The apparent end of the need to retain criminal records did little to temper the collection of them. Instead, a new justification came to the fore: that criminal records would help detectives solve crimes. Such was the speed that this new prevailing thought that by 1915 'criminal record files had become the principal part of the equipment of every detective bureau in Europe'.[162] Vollmer claimed that the ability to properly identify a man and attach his criminal record to him not only encouraged the suspect to plead guilty more readily,[163] but also helped in intelligence gathering because:

> the delinquent changes his demeanour towards [the police] as soon as he learns his identity is known…the defiant attitude vanishes and the hitherto silent and sometimes combative suspect is quite a talkative and congenial sort of fellow, ready to tell all he knows about himself, his associates and his fence.[164]

In light of these renewed foci, the CRO took charge of the vast register of criminal convictions in the Alphabetical Register, joined them to the CSO's old register and renamed it the 'Central Registration Records'.[165] This amounted in 1913 to some 200,000 records.[166] This data was collected for any person who was convicted of any offence by the assizes, the quarter sessions or the court of summary jurisdiction which resulted in a sentence of one month imprisonment or more.[167] These were submitted to them by local forces and prisons, who then input the data into the collection.[168] This conviction data was supplemented by fingerprint identification data – the inclusion of anthropometric data by now abandoned[169] – which ensured the correct record was attached to the correct

[160] Above n.158,1353
[161] Above n.33, 22
[162] Above n.91, 317
[163] Above n.114, 322
[164] Ibid
[165] Above n.4,15
[166] Above n.91, 328
[167] C. Matthews, *The Police Code and General Manual of the Criminal Law* (15th edn, Butterworths and Co 1912) 51 – 52
[168] Above n.166
[169] Ibid, 368

offender.[170] The process was now much more efficient: in 1913, the number of positive identifications was 10,677.[171]

The CRO's extensive collection of fingerprints led to it being described in 1915 as 'the clearinghouse for all information relating to identification'.[172] Although local forces continued to maintain their own local records, it was claimed that 'for all cases, Scotland Yard is consulted'.[173] The CRO repository consisted of prints supplied to them by prison officials, who took them from prisoners who were either remanded or ultimately convicted and sentenced to a period of one month imprisonment or more.[174] Where a suspect was acquitted after having been fingerprinted, that the prints would be destroyed and 'the person left with a clean sheet, so far as Scotland Yard is concerned',[175] although Fosdick found that 'there are occasional exceptions'.[176] By 1935, this 'Fingerprint Index' contained over half a million records.[177] For those not fingerprinted, photographs were instead taken and a description noted on a 'description form'.[178]

The Central Registration Records, described by one officer as 'a veritable who's who of the criminal world',[179] was a collection of 'hard' criminality data. It was a factual record because a person's convictions, fingerprints and photographic image are factual *per se* – unless falsely recorded or amended in some way, a record of a person's criminal convictions merely lists the offences for which a person was charged, brought before a court and either an admission, or a finding, of guilt made, while a fingerprint indentation is a copy of what is contained on an individual's finger. Likewise, a person's face is factual, intrinsic personal identification data.

All of this data was presumed to assist in the work of detecting offences. Despite Churchill's ambivalence and the failure of supervision, for many, the problem of habitual offenders remained unresolved. It was by now recognised that a small number of recidivistic offenders committed large numbers of offences. This explain why Fosdick

[170] R. Fosdick, 'The Passing of the Bertillon System of Identification' (September 1915) 6 Journal of the Institute of Criminal Law and Criminology 3 363, 363
[171] Above n.93, 75
[172] Above n.91, 327
[173] Ibid, 328
[174] Ibid
[175] Above n.79, 193
[176] Above n.91, 328
[177] Above n.4, 16
[178] Above n.4, 15
[179] Above n.93, 55

believed that: 'the prime requisite in the office equipment of a detective bureau is a criminal record file. The police must be acquainted with the criminal propensities of specific individuals'.[180]

The CRO's attempt to detect crime through the use of the Criminal Registration Records was bulwarked by a secondary system called the 'Central Identification Records'.[181] Data here was divided into four sections. The first was the 'Crime Index',[182] which contained information relating to offenders similar to that originally taken from the old distinctive marks registers[183], but whose central tenet was the *modus operandi* system; the brainchild of Major Llewelyn William Atcherley, the Chief Constable of West Riding Yorkshire Constabulary,[184] who believed that habitual criminals were 'creatures of habit' who 'were inclined to develop, refine and follow behaviour in their crime with which they were comfortable' – their *modus operandi.*[185] Atcherley opened his own 'workable clearinghouse' in Wakefield in 1896 based on this principle[186] which was sufficiently successful that a variation of his system was adopted by the CRO in 1913[187] and it even appeared in revised form in the United States in 1919.[188]

By the 1930's the 'Crime Index' became known as the 'Method Index'.[189] A 'Single Fingerprint Index' was added in 1930. This contained a single fingerprint of anyone convicted of breaking and entering offences.[190] A 'Photograph Collection' was also added for the 'most important criminals listed in the method index', along with a 'Wanted Index' of suspects who had not yet been apprehended: this was 'a comprehensive, central listing of persons wanted for arrest, detention or questioning by the police'.[191] A 'Property Index', which documented items lost or stolen, was also instituted to allow items to be traced to crime scenes and returned to lawful owners if recovered.[192]

---

[180] Above n.91, 316
[181] Above n.4, 16.
[182] Ibid
[183] Ibid
[184] L. B. Schlesinger, *Serial Offenders: Current Thought, Recent Findings* (CRC Press 2000) 123
[185] D. Doss et al, *Economic and Financial Analysis for Criminal Justice Organisations* (CRC Press 2014) 503
[186] Above n.181
[187] Above n.184
[188] A. Vollmer, 'Revision of the Atcherley Modus Operandi System', (August 1919) 10(2) Journal of the American Institute of Criminal Law and Criminology 229, 230 – 235
[189] A. Martienssen, *Crime and the Police* (Penguin 1953) 37
[190] Above n.181
[191] J. Rule, *Private Lives and Public Surveillance* (Allen Lane 1973) 58
[192] B. Thompson, *The Story of Scotland Yard* (The Literary Guild 1936) 222

The Central Identification Records were an attempt by the police to undertake a rudimentary, but systematic, attempt at intelligence gathering and 'offender profiling'.[193] This information is 'soft' police intelligence: information held by the police which is attached to the criminal record held against an individual but which is often not 'factual, but speculative or untested.[194] While 'the police have always collected soft intelligence on people'[195] the CRO were engaged in something altogether different. Here was the collation and retention of data, much of it subjectively ascertained, specifically in order to found an investigation into a crime which had not yet occurred: a form of preventative detective work. This gave rise to a new type of police officer: the bureaucratic officer exhibiting 'an unshrinkable passion for processing statistical information and extolling the value of his work', particularly in curbing the activities of the habitual criminal.[196]

Anxious to avoid the access problems of the past, the CRO opened its repository to officers nationwide by wire, open for enquiries between 9am and 6pm every day.[197] This was claimed to have resulted in some 286,000 total identifications by 1928:[198] a figure which rose in one account to 'little less than 400,000' by 1934.[199] The *Police Gazette* was by 1929 being issued daily as an internal publication disseminated only to the police.[200] This contained details of men arrested, descriptions of wanted men and also details of those convicted in court.[201]

There exist several contemporary accounts of the CRO, written largely by police officers who worked there or by those who were granted access to the office by those who did. Almost universally, these paint a picture of hyper-efficiency, extreme importance and pride. Martienssen described the CRO as containing 'detailed particulars of every known criminal, filed under a system which has done more than anything else to put Scotland Yard ahead of every other police force in the world'.[202] Dilnot enthused about CRO staff

[193] Above n.185
[194] C. Baldwin, 'Necessary Intrusion or Criminalising the Innocent? An Exploration of Modern Criminal Vetting' (2012) 76(2) Journal of Criminal Law 140, 144
[195] T. Thomas, *Policing Sexual Offences and Sex Offenders* (Palgrave 2016) 91
[196] Above n.157, 83
[197] Above n.93, 328 – 9
[198] Above n.79, 193
[199] Above n.192, 219
[200] Above n.79, 202
[201] Ibid
[202] Above n.189, 36

as ‘specialists [who] do their work with cold deliberation and machine-like precision’.[203] Moylan claimed that ‘the identity of an arrested criminal can quickly be determined, and that of the unknown author of a crime can often be arrived at’.[204] Woodhall went even further, stating that ‘the officers become so skilled at their work that, after one examination of a set of prints, they can turn up instantly the past record of the person whose prints they are…they rarely make a mistake’.[205]

This notion of the CRO as being routinely capable of near instantaneous crime detection was encapsulated by the Metropolitan Police as ‘catching thieves on paper’[206] It must be taken with a generous pinch of proverbial salt. The notion that CRO officers were able to identify criminals after a single peruse of a set of fingerprints or that 770,000 possible suspects might be narrowed down to a single man due to a quick search and the knowledge of a single officer stretches the bounds of credibility to an barely tenable degree.

Yet this ‘romanticised view of the CRO’[207] persisted into the 1950s; possible, at least in part, because of the widespread public support afforded the police.[208] This was largely attributable to the BBC’s *Dixon of Dock Green,* whose portrayal of the eponymous P.C Dixon strongly reinforced ‘the quintessential representation of the ideal British bobby’[209] as a benign yet protective force for consensus-based law and order.[210] This afforded the Metropolitan Police sufficient credibility to continue to make claims that CRO officers were so in-tune with their duties that ‘as soon as a crime is reported, they are usually able, without looking at their cards, to name several ‘likely starters’.[211]

The reality, though, was rather different. The generally positive perception of the police of the 1950’s is now generally regarded as little more than a ‘potent myth’.[212] The truth was

[203] Above n.93, 70
[204] Above n.79, 200
[205] E. T. Woodhall, *Secrets of Scotland Yard* (John Lane: The Bodley Head 1936) 133
[206] Metropolitan Police, ‘Catching Thieves on Paper: History and Purpose of the Criminal Record Office and the Police Gazette and it’s supplements’ (MEPO 8/42 1936)
[207] Above n.4, 20
[208] G. Gorer. *Exploring English Character* (Cresset, London 1955) 311
[209] T. Newburn and R. Reiner, ‘From PC Dixon to Dixon PLC: policing and police powers since 1974’ (August 2004) Criminal Law Review 601, 603
[210] Ibid, 604
[211] H. Scott, *Scotland Yard* (Andre Deutsch, Lindon 1954) 125
[212] D. J. Smith, ‘Mr. Lustgarden and the case of the honest copper’ (1998) 8 Oxford Journal of Legal Studies 3 434, 434

that ‘beneath the rosy view that dominated popular perspectives, there was undoubtedly a more sordid reality of corruption and abuse.’[213] A Royal Commission, chaired by Sir Henry Willink, was instituted in 1962 to investigate some of the more lurid claims of corruption and incompetence[214] and many of the 111 recommendations made were implemented by the Police Act 1964. Anecdotal evidence also began to emerge which questioned the supposed efficiency of the CRO. One MP asked the Home Office three times how long it takes for the CRO to trace a fingerprint, and was eventually told that a search could take ‘between ten minutes and five hours’.[215]

This might explain the Home Secretary was moved to admit that ‘the provincial police…do not, in fact, call in Scotland Yard today with the unanimity of which writers…always depict’. In fact, in 1953 they ‘asked for help in seven cases’.[216] The reality was that, despite Parliament pronouncing in 1934 that ‘the system of keeping criminal records is no longer based on regions’,[217] local collections continued to run parallel to the main scheme and, as the CRO grew, so did they. Atcherley’s Wakefield operation was ‘working very successfully’[218] and had become the *de facto* CRO for the north of England.[219] Prior to the outbreak of the First World War, a clearing house had been instigated in Birmingham.[220] In Scotland, eleven different forces had established their own smaller version of the National CRO.[221] A response to a Parliamentary question confirmed in 1933 that the forces of South Wales, Gwent and Dyfed-Powys Police had made ‘joint arrangements’ for the collection, retention and use of their own collection of criminal data.[222]

In 1938, the Home Office recommended that regional ‘clearing houses’ be instituted in Liverpool, Cardiff and Bristol, so long as these continued to formally recognise the primacy of the national CRO at Scotland Yard.[223] Thomas claims that ‘informally, this was a recognition of continued problems in accessing the London records and the unreliability

[213] Above n.209
[214] H. Willink, ‘Royal Commission on the Police, Final Report’ (Cmnd 1728 1962)
[215] HC Deb 23 June 1966, vol.730, col.877
[216] HC Deb 6 May 1954, vol.527, cc.583 – 645, col. 635
[217] HC Deb 20 July 1933, vol.46, col.141W
[218] G. Glover Alexander, *The Administration of Justice in Criminal Matters (in England and Wales)* (Cambridge University Press 1915) 223
[219] P. J. Stead, *The Police of Britain* (MacMillan 1985) 77
[220] ‘Sessional Papers, Volume 22’ Report (HMSO 1920) 111
[221] Above n.4,18
[222] Above n.189, 37
[223] Above n.4, 20

of their content'.[224] Whatever the explanation, in 1952 a working group of chief constables presented the Home Office with a report which recommended the formal recognition of regional criminal records collections.[225] The result of this was that during the 1950's and 1960's a number of Regional Criminal Record Offices ('Regional CROs') were set up.[226] By 1956, the Wakefield operation had been converted into a Regional CRO, as had that in Birmingham, and another six had opened by 1959. [227] A Scottish CRO was opened in Glasgow in April 1960.[228]

A fairly detailed account of the workings of the Birmingham Regional CRO (or 'Mid-cro', as it was apparently known by police)[229] was provided in the *Police Journal* in 1961. Some sixteen forces were said to contribute to the records held there,[230] which oversaw a geographical area of around 100 miles and a population of around 5.5 million.[231] Mid-cro operationally mirrored the National CRO; they operated five main collections of records: court convictions, a method index, a fingerprint index, a stolen property index and a photograph collection.[232] The main collection of criminal records by 1961 held 75,371 records. Most of these were 'fresh' records: records of individuals who had come to the attention of the police in the previous five years.[233] Around 100,000 fingerprints had been taken and retained.[234]

Information was passed between the Regional CROs and the National CRO by facsimile machine, which was installed at all of the CRO offices. This allowed for photographs and fingerprints to be sent and checked more quickly.[235] The dissemination of information from the National CRO continued by publication of the *Police Gazette* and *Informations*, though this was restricted to crimes and criminals with 'national importance'.[236]

---

[224] Ibid, 19
[225] Ibid, 21
[226] I. Kroener, *CCTV: a technology under the radar?* (Routledge 2014) 40
[227] Above n.4, 24
[228] A.G. Ralston, *The Real Taggarts: Glasgow's Post-War Crimebusters* (Black and White Publishing 2017)
[229] 'Regional Criminal Records' (1961) 34 Police Journal 310
[230] Ibid
[231] Ibid, 310 – 11
[232] Ibid, 311
[233] Ibid
[234] Ibid
[235] J. D. Devlin, 'Procedure, Administration and Organisation: VI Police Communications', (1966) 39 Police Journal 620, 622
[236] J. D. Devlin, 'Procedure, Administration and Organisation: IV Police Communications', (1966) 39 Police Journal 514, 518

2.5 James Rule's account of the CRO system

Between April 1970 and December 1971, the Metropolitan Police and several of the Regional CROs gave American academic James Rule extensive access to the workings of the CRO system. Rule's seminal account[237] of what he saw cast such doubt on the rose-tinted accounts proffered by police officers that the Home Office commented pre-publication that substantial portions should be 'left out' and 'fundamental changes' be made to others.[238]

Rule described each criminal record folder as consisting of three main forms. The first was 'the criminal record file'. This was a list of all recorded convictions against an individual – offence description, date, court and sentence.[239] The second was the 'descriptive form', completed every time a person was charged with an offence and containing a description of the alleged offence, the circumstances of the arrest and a physical description of the individual (including a photograph).[240] The third was an 'antecedent history': an abridged summary of relevant factors which the police subjectively believed to be relevant to an offender and their offending. Almost as standard, this would make reference to the offender's place of residence, his family circumstances, education, financial situation, employment status and history and known associates.[241]

Almost identical records were available at the Regional CROs, although the files may include additional information – some CRO's included press clippings of offenders in their files, for example,[242] while others also included 'notes' compiled by the police when investigating an individual for a subsequent offence. Rule was unable to provide substantial detail on these, as the police were 'often chary about discussing them'.[243] Moreover, regional files would ordinarily only contain information on convictions obtained in the geographical ambit of the Regional CRO.[244] The net result was that files held at Regional CROs were not uniform, with some forces maintaining very up-to-date and detailed files on known offenders, but others only updating files when convictions were secured.[245] Rule also noted that individual CIDs at police stations had their own 'local'

[237] J. B. Rule, *Private Lives and Public Surveillance* (Allen Lane 1973) 44 – 96
[238] Ibid, 95
[239] Ibid, 50
[240] Ibid
[241] Ibid, 51
[242] Ibid
[243] Ibid
[244] Ibid, 68
[245] Ibid, 56

records, on which they kept whatever information on offences and offenders their felt appropriate, in whatever form they deemed necessary.[246]

The problems with such an enormously fragmented information-sharing system were highlighted in vivid clarity. The use of criminal record files in the bringing of a prosecution clearly involved a significant bureaucratic process. The process commenced by completing the descriptive form and sending this by courier to the National CRO and which ended with the file being returned with a new conviction added to it was nowhere near as quick as police had claimed. In fact, it expended a lot of labour and an enormous amount of time.[247] For example, the time taken for Regional CROs to send a descriptive form and fingerprints to the National CRO, get these checked, and have the necessary information returned to them was 'at least a week, and often more'.[248] This was because National CRO staff were so busy dealing with enquiries relating to the Wanted and Missing Persons Index (a list of some 65,000 persons either missing and those wanted by law enforcement agencies for outstanding matters and deemed priority)[249] that they often could not process requests on the criminal record files in good time, or even at all; Rule saw one check was returned and marked 'no trace' (i.e. no record held) on a man known with certainty by the Regional CRO to have a criminal record.[250]

These delays were, in essence, the justification for having Regional CROs despite the obvious duplication in their work. Regional CROs were at least were able to provide some data 'within the day of receipt' and were used instead where 'a record' had to be brought at short order to the Magistrates Court.[251] The problem with that 'solution' was that an offender might have numerous convictions listed under their name at different Regional CROs and, where this occurred, these records would likely be incomplete. Rule observed that communications between Regional CROs to allow for such records to be synchronised was 'not strictly adhered to, especially given the difficulty of determining a criminal's place of residence'.[252] Even where efforts were made to record all convictions, things did not 'work perfectly…and some convictions go unrecorded'.[253]

[246] Ibid, 77
[247] Ibid, 64 – 66
[248] Ibid, 69
[249] Ibid, 58
[250] Ibid, 69
[251] Ibid, 64
[252] Ibid, 68
[253] Ibid, 66 – 67

In short, even the supposedly 'complete' national records were not so. Rule confirmed David Steer's earlier work which found a significant variance between forces, with one force reporting 98% of convictions to the National CRO but another reporting only 68%.[254] Steer believed this reflected a reluctance on the part of the police to report offences where the offender was not fingerprinted: this was only undertaken at the time when an offender was arrested and charged with an offence by the police, rather than summonsed by a magistrate.[255] In a later study, after the fingerprinting rules were amended, Steer found that around 96% of all convictions were being reported to the CRO.[256] While this certainly reflected an improvement on his study a decade earlier, this still meant that the supposed 'definitive' record was incomplete.

Attempts to manage the scale of the collections also involved the destruction of records. Descriptive forms and other records relating to an offence were usually destroyed if the accused was subsequently acquitted,[257] though this practice was not uniformly undertaken, with some Regional CROs retaining photographs of those acquitted where these 'updated' an existing file, while others retained fuller records if the acquittal related to especially serious allegations, particularly sexual offences.[258] Processes were also in place to delete old, inactive records: a process described as 'weeding'. In 1970, 46,000 records were 'weeded' at the National CRO, though Rule felt this was likely a result of staff coming to files suitable for weeding, rather than any conscious effort to search systematically for them. The latter, he contended, was not practical for lack of manpower.[259]

2.6 Conclusions

By 1973, alongside the national collection of records held at the National CRO, there not only existed nine other collections maintained by Regional CROs and those maintained at the 'Group Record Offices' but also locally held record collections at each of the forty-seven police forces. This, according to James Rule, resulted in a 'pyramid of information exchange': the National CRO providing the authority at the top, the regional offices

[254] D. Steer, 'The Elusive Conviction' (1973) 13 British Journal of Criminology 373, 376
[255] Per s.40 of the Magistrates Courts Act 1952, repealed by s.33 of the Criminal Justice Act 1967
[256] D. Steer, 'Recorded Convictions' (1971) University of Oxford Penal Research Unit pp.8a – 8c
[257] Above n.91
[258] Above n.237, 67
[259] Ibid at 71

working in collaboration with it and each other to provide information to police 'users' at the base.[260]

At the turn of the twentieth century, it was intended that the Criminal Records Office in London would form a central 'clearinghouse' for crime and criminals. What is clear from the conscious process of decentralisation and fragmentation which came in the 1950s and 1960s was that this notion had failed. This failure was apparent seemingly to all parties: the police were calling for the 'regionalisation' of criminal records by 1961,[261] the development by National CRO staff of the 'District 6' operation showed that they were no less desirous of decentralisation than anyone else and Parliament's complicity in the Regional CROs seemed to acknowledge they had come to a similar conclusion. If further evidence were required, the implementation of the Criminal Law Act 1967 to 'repeal obsolete or unnecessary enactments',[262] included the repeal of ss.6 – 7 of the Prevention of Crimes Act 1871, formally removing from the statute books a requirement on the police to make a central record of offenders. This meant that, from 1967, there was no statutory basis for the collection of criminal records at all.[263]

Why did centralisation fail? The answer appears to lie in a combination of factors. Firstly, the sheer volume of records at the National CRO had grown to an almost unmanageable level. By 1960, when many of the Regional CROs had been instituted, demand on the National CRO was enormous; 733,104 searches were conducted against their records that year, an increase of over 67,000 on the previous year and an additional 226,301 convictions were added to the records. [264] In the same year, 40,924 motor vehicles were added to the property index as having been stolen and the Police Gazette circulated details of 12,821 cases.[265] By 1970, the National CRO were adding half a million new records to their files, and were in possession of a total of around 2.5 million criminal records.[266] This was an enormous collection – far greater than that originally envisaged by the originators of the 'national clearinghouse' notion, when it was said that 'it might

[260] Above n.237, 44 – 45
[261] W. Palfrey, 'Police Communications' (1961) 34 Police Journal 79
[262] Criminal Law Act 1967, Schedule 3, Part I,
[263] C. Baldwin, 'The Vetting Epidemic in England and Wales, (2017) 81(6) Journal of Criminal Law 478, 480
[264] 'Report of the Commissioner of the Metropolis for the Year 1961' (Cmnd 190, HMSO 1961) 68
[265] 'Sessional Papers, Volume 20' (HMSO 74 1961)
[266] Above n.191, 67

reasonably be foreseen that it is not likely to exceed half a million, and may possibly be kept down to nearer 400,000'.[267]

The problems with such an extensive collection are, at least in part, fairly self-evident. The collation of so much data using paper and card indexes meant that individual records were enormous – one officer described in 1962 that 'a CRO file is almost a biography'[268] – and the storage of two and a half million enormous 'biographies' required a full floor of New Scotland Yard.[269] It is obvious that very large collections of manually held criminal records 'cannot be maintained with the same speed and accuracy' as smaller ones and by 1971 the National CRO alone employed over 400 staff.[270] Operational problems also inevitably followed: the dissemination of information from such a vast collection was inevitably slower than it might have been. Regional circulation information was much quicker.[271] Moreover, regional collections could be tailored to retain information directly relevant to the local force(s): local stolen property indies could contain details not deemed worthy of record at national level, for example.[272]

By the early 1970's, then, the notion that the CRO at Scotland Yard would form a national 'clearing house' for crimes and criminals appeared to have died. Detectives still wanted access to criminal records to help them solve crimes, but they needed it quicker and more individually tailored than the National CRO could provide. The process of decentralisation and fragmentation was so complete, and the problems so endemic to the criminal record collection process, that it seemed that only computerisation of the criminal records, if possible, might bring the records back to a centralised collection of value to operational policing.

[267] Above n.79, 197
[268] R. Barr, *The Scotland Yard Story* (Hodder and Stoughton 1962) 17
[269] Above n.191, 44
[270] Ibid, 47
[271] Above n.135, 518
[272] Ibid

3
PHOENIX

3.1 Introduction

With the notion of a hyper-efficient CRO presiding over a 'British library of crime and criminals' exposed as a myth and the reality of the Metropolitan Police struggling to effectively collate, store and manage literally millions of hard-copy 'biographies' of known offenders now in the public domain, attention turned to affecting a solution which would allow the police to continue to use criminal records to help investigate offences. By 1970, the obvious solution appeared to lie in computerisation

This chapter will examine the path towards the computerisation of the national criminal record collection and the exponential increase in records retained that this brought. Explanations for the expansion will be sought, and critical comment on what purported policing aim this sought to achieve, and whether increased collection furthered those aims, will also be offered. Ultimately, it is intended that this chapter will decisively address the first research question; identifying what, as matter of literal fact at least, the police are retaining in their 'criminal records' so that an accurate definition might be offered in the concluding chapter of this thesis.

3.2 The Police National Computer ('the PNC')

As has been seen, the CRO was operating in 1970 largely in the same way it was in 1913. The benefits of computerisation were obvious to the Metropolitan Police by the 1960s; envious comparisons with computerised systems newly installed in the United States noted that:

> The equipment the police have in the present day can only be described as archaic. In the whole of Britain there is not a single computer or data processing machine in use by the police. A single fingerprint may take ten men six weeks to find. A computer in New York can compare 100,000 fingerprints in three hours…The police must have this sort of equipment'.[1]

[1] T. Jeanes, 'Police Note' (Nov. 1965) Bracton Law Journal 15, 16 – 17

In fact, preliminary research into the possibility of computerising the various police record collections (including the CRO's) began in 1964[2] and the Home Office formally notified the police of their intentions in December 1965.[3] By 1967 the project was being openly discussed in Parliament: Lord Stonham telling the House of Lords that the Government intended to provide 'direct and immediate' access to everything being held manually at the CRO's: names, lists of previous convictions, *modus operandi*, fingerprints and the Wanted and Missing Persons Index.[4] By 1969, the Home Office invited the police into the consultation process,[5] then on 28 January 1970 the Home Secretary formally announced plans to purchase and install the Police National Computer[6] at a cost of around £16m.[7] This was an official recognition that the entire CRO system was suffering from 'very considerable problems'.[8]

Ministers explained that the PNC would allow officers 'on the beat' to radio requests for information to colleagues who, using video display terminals, would be able to access it near instantaneously and return the requested intelligence.[9] Each police force was to be equipped with at least one terminal and 600 specialist officers were trained to use it.[10] It was expected that the system would be operation by 1972. In fact, the PNC did not 'go live' until 1 April 1974 and in the initial phase only the national file of stolen motor vehicles was added to it.[11] This allegedly reduced the time required to make a check 'from ten days to a matter of a few seconds'.[12]

While such hyperbolic statements ought reasonably be treated with a degree of suspicion, it is clear that the PNC was a new and 'incredibly powerful tool'[13] which was 'revolutionary in its impact and arguably represents the single most important contribution of the Home Office to policing in this country since the creation of the Metropolitan Police in 1829'.[14]

---

[2] S. R. Walker, 'The Police National Computer Records' (1970) 43 Police Journal 111, 113
[3] T. Thomas, *Criminal Records: A database for the criminal justice system and beyond* (Palgrave MacMillan 2007) 27
[4] HL Deb 29 November 1967, vol. 287, col. 141
[5] Above n.3
[6] Above n.2,111
[7] Ibid at 112
[8] HL Deb 18 February 1970, vol.307, col.1179
[9] Above n.6
[10] T. Brain, *A history of policing in England and Wales from 1974: a turbulent journey* (Oxford University Press, 2010) 9
[11] HL Deb 31 October 1974, vol.374, col.169
[12] Ibid
[13] Above n.10
[14] Ibid.

The police quickly began adding more of their data collections to the PNC. The CROs fingerprint collection went live in 1976.[15] This amounted to the uploading of 2,484,437 sets of fingerprints.[16] By the end of 1977, the entire DVLA database of vehicle ownership – 17.7m records – had been added to the PNC.[17] This required additional resource to maintain; the 'PNC Unit' at Hendon, which maintained the PNC, by now employed about 450 staff[18] and the cumulative cost to this point to the Home Office was almost £15m.[19]

Yet there was no attempt to upload the criminal record collection. In 1977, a 'Names Index' (now the 'nominal index') application was added. The Home Office claimed in December 1977 that this listed some 3.8 million individuals.[20] The Names Index was not a 'criminal record database', though – it was simply a list of those individuals against whom paper records were held at a CRO, warning officers that the individual in question had a criminal record.[21] A year later, the 'Index of Wanted and Missing Persons' was added.[22] Checks against this index were long considered a priority for police and CRO staff[23] and remained so due to officers' use of so-called 'stop-check' searches; an officer on the beat encountering a suspicious individual and asking for a check on whether s/he was wanted for any offence.[24] The PNC must undoubtedly have improved the speed of such checks and freed up resource at the CROs.

By 1980, the PNC held 19 million vehicle registrations, 3.25 million fingerprint sets and 3.8 million criminal names. The system was handling almost 11 million requests for information on individuals, mostly made by police officers on the street.[25] Yet it still contained not a single criminal record. The decision not to include the criminal records in the early tranche of uploads has never been publicly explained, but it is submitted that the decision simply must have been taken that the information contained in the criminal records was no longer considered an operational priority.

---

[15] B. Harrison, *Finding a Role? The United Kingdom 1970 – 90* (Oxford University Press 2011) 476
[16] 'Fingerprints', HC Written Answers 7 May 1976, vol.91
[17] 'Police (Records)', HC Written Answers 2 December 1977, vol.940
[18] 'Computers', HC Written Answers 7 July 1977, vol.934, col.629
[19] Ibid at col.631
[20] Above n.17
[21] Above n.3
[22] D. Wilson, *Surveillance, Crime and Social Control* (Routledge 2006) 4
[23] J. B. Rule, *Private Lives and Public Surveillance* (Allen Lane 1973) 61
[24] Ibid, 62
[25] E. Higgs, *The information state in England* (Palgrave MacMillan 2004) 179

Meanwhile, in 1980, the National CRO was renamed the National Identification Bureau.[26] It is submitted that this provides further insight into the use of the criminal record repository at this time; the testimony of police officers extolling the virtues of criminal records as a crime prevention and detecting tool seemed to have dried up and the focus instead was on using records as means of identifying individuals stopped, checked and brought into custody, and little more. In 1980, new technology was finally brought to bear on the national collection of criminal records, but instead of being added to the PNC, the decision was taken to convert the National CRO records to microfiche.[27] New convictions were reported to the NIB by local forces and then added by NIB staff to the records. Only recordable offences were listed – i.e. any offences which might potential incur a prison sentence.[28]

In 1985, work finally began on adding some criminal records to the 'Names Index'; where an individual was convicted of a new recordable offence on or after 1 January 1981, the entire National CRO record held against that person (if any) was subsequently added.[29] This proved problematic: the PNC was by this point almost operating at full capacity; by October 1991, the PNC held just over 39.57 million vehicle records, 4.3 million fingerprint records, just under 5.4 million criminal names and 3.95 million conviction records.[30] Plans were announced to upgrade to a new system ('PNC2'). To help fund the upgrade, suggestions were made by the Conservative government to privatise the new system, though this was ultimately rejected amidst concerns over confidentiality and security.[31] PNC2 was intended be approximately ten times more powerful than its predecessor.[32] Consisting of 2,600 terminals, 200 printers and 4 police local computers,[33] it was originally intended to go online at the end of 1990[34] but the system went 'on-stream' in stages and the criminal names, fingerprints, wanted and missing persons, disqualified drivers and convictions data were migrated and operational by November 1991.[35]

[26] Above n.3, 25
[27] Ibid
[28] Ibid
[29] Above n.3, 28
[30] 'Police National Computer', HC Written Answers 22 October 1991, vol.196, col.530
[31] HC Deb 7 December 1989, vol.163, col.461 – 62
[32] HC Deb 18 October 1991, vol.196, col.598
[33] Above n.3, 29
[34] 'Police Computer' HC Written Answers 24 July 1990, vol.177
[35] 'Police National Computer', HC Written Answers 29 November 1991, vol.199, col.657

More organisations were given access to the 'police' national computer; 'read only' access to the system was granted to the Home Office, HM Customs and Excise and the DLVA and proposals to give access to 'other Government Departments' were being considered by ministers.[36] Local authorities were also now 'pressing hard' for access to the system.[37] The size of the collection continued to grow: now 4.2 million convictions[38] were stored, along with 4.3 million fingerprints and 5.5 million criminal names and disqualified drivers.[39] It was claimed that the PNC was now 'an established part of police operations…now as much part of the police back up as the police car and police radio. It is a tool to help police officers investigating and detecting crime and bringing offenders to justice'.[40]

3.3 PHOENIX – the 'Criminal Justice Record System'[41]

Some seventeen years since the PNC came online, the national collection of criminal records were still not computerised. The impetus to finally computerise the collection came when the problems with the hard-copy records at the NIB became sufficiently well publicised that it was impossible to ignore them. A Scrutiny Committee appointed to investigate the situation[42] found that the criminal record collection was 'in a very unsatisfactory state'.[43] It recommended that a new approach, tailored towards the entire criminal justice system, be taken.[44] Records should be computerised to PNC2 and that the Regional CRO's, which cost £2.5m a year in staffing costs alone, would become superfluous and should close.[45] It also suggested that a new central agency be created to control the collection and that the new agency be able to charge for access to users, including the police.[46]

While the Government eventually rejected the notion of creating a new, fee-charging agency to look after the records, it did agree with computerising them and work began on the new PNC2 application required to accommodate them. In 1992, the Home Office told

[36] 'Police Computer', HC Written Answers 15 October 1992, vol.177, col.719
[37] 'Police National Computer', HC Deb 3 February 1992, vol.203, col.105
[38] Note – 'convictions', not 'criminal records'. Each offender counts as one entry on the nominal index but may have tens, or even hundreds, of convictions.
[39] 'Police National Computer', HC Written Answers 7 July 1992, vol.211, col.126
[40] HC Deb 3 February 1992, vol.203, col.109
[41] Home Office, 'PHOENIX, Putting you in the picture' (London: Police Department, Science and Technology Group 1995)
[42] Home Office, 'The National Collection of Criminal Records: Report of the Efficiency Scrutiny' (HMSO: London 1991)
[43] Ibid, para.19
[44] Ibid, para.23
[45] Ibid, para.48
[46] Ibid.

Parliament finally announced formal plans to transfer the entire NIB criminal record collection to PNC2; confirming the widened scope for the records, the Home Office told Parliament that:

> [The] national criminal records system will become an indispensable aid to the better functioning of the whole of the criminal justice system. It will be of significant benefit to the police in investigating and detecting crime. Comprehensive and accurate information on antecedent offences will assist in the prosecution of cases and in sentencing, and it will help the prison service to determine the appropriate prison regime.[47]

This new PNC application was to be called the 'Police Home Office Extended Names Index', or PHOENIX. The inputting of criminality information onto PHOENIX would be done locally, by police officers using PNC terminals, rather than by the NIB.[48] The Regional CROs were, as recommended, closed. The Government put to tender the contract for converting the back-record collection to PNC and eventually awarded the contract to PCL Group on 5 July 1994 for the conversion of three million records microfiche records over eighteen months[49] at the cost of £8.8 million.[50]

PHOENIX 'went live' on 22 May 1995 and, on the same date, the NIB was renamed the National Identification Service ('NIS').[51] PHOENIX replaced the 'Names Index' and includes a description of the individual listed, details of offences alleged or committed by that individual and details as to whether the individual was reported as 'missing' or 'wanted' or a 'disqualified driver'.[52] it listed some 5.3 million criminal histories and over 17 million searches were being made annual against the PHOENIX application alone.[53] The principal advantage of PHOENIX was that individual officers could immediately access and update criminal details from any of the 10,000 terminals provided to police forces, while others granted 'read only' access to it could view the data required equally quickly.[54]

---

[47] Above n.40
[48] Above n.3, 36
[49] 'Computer Contracts', HC Written Answers 8 July 1994, vol.246, col.331
[50] 'Criminal Records Database', HC Deb Written Answers 5 November 1996, vol.284
[51] Above n.3, 37
[52] Above n.48
[53] 'Police National Computer', HC Written Answers 7 June 1995, vol.261, col.185
[54] Above n.48

Court staff would pass disposals information directly back to police forces for PHOENIX input.[55] This removed the remit of the NIS to centrally maintain the criminal records.

PHOENIX remains the PNC application where criminality data stored and continues to be used in largely the same manner with which it was introduced in 1995, save that it now also includes information on individuals who have been granted firearms licences and those who have 'certain court orders made against them'.[56] What is notable, though is that volume of criminal records has grown exponentially: in 2008, PHOENIX contained over 8.6 million records,[57] by 2014 the total had reached 10,520,929[58] and the total number of criminal records at September 2017 was 11,166,266.[59]

The research to this point has sought to ascertain what, historically, the state and the police have collated under the banner of 'criminal records'. The purpose of the remainder of this chapter is to attempt to identify what criminality data the police are capturing on PHOENIX and whether these offer any explanation for the growth in the volume of records collated. In doing so it is intended to offer a contemporary analysis of what the police now are collating under the banner of 'criminal records' and, per the first research question, to identify whether the notion of criminal records as a collection of court convictions stands scrutiny.

[55] S. Mason, 'A common sense approach: a review of the criminal record regime in England and Wales (Report of phase two)' (Home Office 30 November 2011) 10

[56] See Home Office, 'Police National Computer (PNC) Guidance (version 5.0)' (23 January 2014) 7. Presumably these refer to non-conviction orders such as Anti-Social Behaviour Orders, Criminal Behaviour Orders, injunctions, restraining orders and suchlike which might feasibly be of interest to police and criminal justice agencies

[57] National Policing Improvement Agency, 'Memorandum by the National Policing Improvement Agency' (NPIA December 2007) presented to the Constitution Committee, *Surveillance: Citizens and the State* (HL 2008 – 09, 18–I) para.6

[58] Home Office, 'FOI Release. Nominal Criminal Records on the Police National Computer' (FOI release 33517, Gov.UK 21 January 2015) <https://www.gov.uk/government/publications/nominal-criminal-records-on-the-police-national-computer> accessed 15 May 2019

[59] Home Office, 'FOI Release. Number of nominal records on the Police National Computer' (FOI ref 44921, *What Do They Know?* 27 October 2017). <https://www.whatdotheyknow.com/request/number_of_nominal_records_on_the#incoming-1060100> accessed 15 May 2019

3.4 The PHOENIX criminality data: what the police are collecting

PHOENIX is not merely a repository of criminal matter disposal information. Offence details, bail conditions, 'warning signals',[60] *modus operandi* and distinguishing marks are just some of the other criminality data retained by the police on PHOENIX[61] The retention and use of this so-called 'soft information/soft intelligence'[62] are subject to various important criticisms which are largely outwith the subject of this research.[63] However, the bulk of the PHOENIX repository relates to the disposal of criminal matters as they progress through the criminal prosecution process in England and Wales; the traditional concept of 'a criminal record'.[64] A detailed examination of what is being stored is offered below:

3.4.1 Non-conviction data

An individual has no record against them on PHOENIX until or unless they are arrested. Only once an individual is arrested will officers create a 'nominal record' containing the personal details of the arrestee and details of the alleged offence(s) against them. The record is marked 'CJ Arrestee' ('Criminal Justice Arrestee'), so that officers accessing PHOENIX can differentiate between those convicted of offences and those not.[65]

If an arrest results in a police decision to take 'no further action' ('NFA'), a charge which results in a discontinuance prior to trial, or if the individual is ultimately acquitted, then the record is not deleted; the nominal record is simply retained on PHOENIX and the non-conviction disposal moved to a file marked 'Event History'.[66] A formal Policy issued by the National Police Chief's Council ('the NPCC') in 2015 states that 'an Event History will be recorded even though an individual has come to the attention of the police on

[60] These have proven controversial since their existence became known: it was revealed (see D. Campbell and S. Connor, *On the Record – Surveillance, Computers & Privacy* (Michael Joseph 1986)) in the 1980's that markers included 'mental' (for those suffering mental health issues) and 'alleges' (makes false allegations of the police) while the Data Protection Registrar was moved in 1993 to intervene on the retention of HIV/AIDS warning markers (Data Protection Registrar, 'The ninth report of the Data Protection Registrar' (HMSO June 1993)). Whilst important, critical evaluation of the use of 'markers' lies outwith the scope of this research.
[61] K. Povey, 'On the Record: Thematic Inspection Report on police crime recording, the Police National Computer and Phoenix Intelligence System data quality' (HM Inspectorate of Constabulary July 2000) 132 and also Home Office, 'The PNC User Manual, v.15.02' (December 2015) 10
[62] T. Pitt Payne, 'Employment: the shadow of the past' (6 November 2009) 159 New Law Journal 1530
[63] See, for example, C. Baldwin, 'Necessary intrusion or criminalising the innocent? An exploration of modern criminal vetting' (2012) 76 Journal of Criminal Law 140
[64] T. Thomas, 'Criminal record of police record?' (3 November 2000) 150 New Law Journal 1629
[65] National Police Chiefs Council, 'Deletion of Records from National Police Systems' (2015), para.1.5.4
[66] Ibid, para.1.5.3

one occasion and regardless of whether that resulted in the person being convicted of an offence'.[67]

It is, therefore, perhaps more accurate to describe PHOENIX as a national collection of individuals *arrested*, rather than a collection of *criminal convictions*. The inclusion and retention of all arrests will inevitably lead to an increased number of records; it is self-evident that there are more people arrested in total than there are people cautioned or convicted of offences and the number of individuals included on PHOENIX would be immediately reduced if such records were not retained.

3.4.2 Reprimand and Warnings[68]

The Crime and Disorder Act 1998 divested upon the police legal authority to issue reprimands and final warnings under the 'Final Warning Scheme' ('the FWS'), which provided that, except where the offence was so serious that the juvenile must be immediately charged, the suspect should be reprimanded for a first offence, given a final warning for a second and charged for a third.[69] Among the pre-conditions for issuing the reprimand or a final warning, the juvenile must have made a clear and reliable admission of guilt to an offence, have no prior convictions and there be no public interest in a prosecution.[70]

The FWS was designed to be reformative, rather than punitive[71] and neither a reprimand nor a warning carried immediate punitive sanction.[72] Warnings and reprimands were always issued in private[73] and were therefore not a matter of public record.[74] They were not designed to be,[75] nor are they legally considered, a conviction[76] while statutory guidance issued in 2001 reassured police that reprimands and warnings

[67] Ibid, para.1.6.7
[68] Authorised by para.3(1)(b) of the National Police Records (Recordable Offences) Regulations 2000 SI 2000/1139
[69] Home Office, 'Final Warning Scheme: guidance for the police and youth offending teams' (Home Office Communication Directorate November 2002), para.4.4
[70] Per section 65(1) of the Crime and Disorder Act 1998
[71] *R v Durham Constabulary ex. Parte R (FC)* [2005] UKHL 21 [4] (Lord Bingham)
[72] Ibid [6]
[73] Above n.69, para.9.20
[74] *The Queen (on the Application of R) v The National Police Chiefs' Council and others* [2017] EWHC 2586 [58] (Justice Green)
[75] Above n.69, para.12.13
[76] Above n.71 [14]. In Lord Bingham's view, the key determination was that neither a warning nor a reprimand incurred any immediate punitive element: 'The determination of a criminal charge, to be properly so regarded, must expose the subject of the charge to the possibility of punishment, whether in the event punishment is imposed or not'.

did not constitute a criminal record.[77] Encouraged by the Home Office to engage with the FWS, and reputedly in favour of it themselves,[78] the police duly issued hundreds of thousands of reprimands and warnings; in 2006 – 07 alone, some 127,326 were issued.[79]

Restorative justice projects are routinely accused of net widening,[80] but it is submitted that such an accusation against the FWS is well-founded. Notwithstanding the police's initially support for the scheme, which facilitated greater engagement with it, they also found themselves required to meet new Government 'key performance indicators', which (perhaps inevitably) discouraged them from using the kind of 'informal warnings'[81] which had been traditionally used[82] to deal with juvenile offending:[83] Quite simply:

> A lot of police officers don't deal with things that way because we're performance led, we're performance driven, therefore an arrest for burglary is a performance figure because this is rammed down our throats 24 hours a day.[84]

Even where the police felt able to use informal disposals, official guidance made it clear that police retained only 'strictly limited discretion to take informal action' and that 'informal action should be taken only in exceptional circumstances'.[85] This was a marked shift in direction from previous policy, which had encouraged forces to divert children out of the criminal justice system by means of informal warnings, words of advice or by taking no action at all,[86] and meant that the 'first formal step on the ladder, the reprimand', is becoming a routine response even for very trivial offences';[87] for

[77] Home Office,' Final Warning Scheme' – Guidance for Police' (April 2000), para.75
[78] I. Walters, 'The Policing of Young Offenders' (2007) 47(4) British Journal of Criminology 635, 648 – 49
[79] Ministry of Justice, 'Criminal justice statistics quarterly: December 2012' (30 May 2013) table A2.4
[80] A. Morris, 'Critiquing the Critics' (2002) 42(3) British Journal of Criminology 596, 602
[81] S. Field, 'Early intervention and the 'new' youth justice: a study of intensive decision making' (2008) 3 Criminal Law Review 177, 181
[82] K. Puech and R. Evans, 'Reprimands and warnings: populist punitiveness or restorative justice?' (October 2001) Criminal Law Review 794, 796
[83] T. Bateman, 'Youth Justice News' (2007) 7 Youth Justice 66
[84] Above n.81
[85] Above n.69, 8 with emphasis in the original. This position was largely reiterated in 2006: see Home Office, 'Circular 14/2006, The Final Warning Scheme' (17 May 2006), para.14
[86] R. Evans and C. Wilkinson, 'Police cautioning of juveniles: the impact of the Home Office Circular 14/1985' (March 1990) Criminal Law Review 165
[87] Above n.81,179

example, between 2002 and 2006, 98 children were warned or reprimanded for attempting to purchase alcohol.[88]

It is submitted, in fact, that the FWS became a system with 'a never-ending reach'.[89] One study found that the number of children being processed by the criminal justice system increase by 11.4% from 2001/2 to 2005/6.[90] Individual instances of possible net widening are evidenced in subsequent litigation; a warning issued to an 11 year old boy in relation to the theft of a bicycle[91] and reprimands issued to four 12-year-old girls for jointly stealing a £20 sarong.[92]

The police and the government eventually became disenchanted with the FWS[93] and it was abandoned in 2012[94] by which time well over half a million reprimands and warnings had been issued,[95] all of which to children[96] and many of which would have been dealt with informally in the years immediately preceding the implementation of the FWS. By 2002, the Home Office had abandoned the pretext that these did not constitute part of a criminal record; [97] each warning or reprimand meant a nominal entry onto the PHOENIX application, accompanied by photographs[98] and fingerprints.[99]

3.4.3 Cautions [100]

An adult caution is 'a formal warning that may be given by the police to persons aged 18 years or over who admit to committing an offence'.[101] Referred to since their inception as 'police cautions' or 'formal cautions', these are now properly referred to as

[88] HL Written Answers 3 November 2008, vol.705, col.3WA
[89] B. Goldson and J. Muncie, *Youth Crime and Justice* (Sage 2006) 216
[90] M. Telford, 'Youth justice: new shoots on a bleak landscape – Director of Public Prosecutions v P' (2007) 19(4) Child and Family Law Quarterly 505, 506
[91] *R (on the Application of T and another) v Sec. of State for the Home Department* [2014] UKSC 35 [4] (Lord Wilson)
[92] Above n.74 [21]
[93] F. Done, 'Youth Cautions: keeping children out of court' (2012) 176(47) Criminal Law and Justice Weekly 678
[94] This was done by statute: the system was repealed by section 135 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012 which repealed s.65 – 66 of the Crime and Disorder Act 1998. After this point the police were not permitted to issue any further warnings or reprimands.
[95] Ministry of Justice, 'Youth Crime: Young People aged 10 – 17 receiving their first reprimand, warning or conviction, 2000–1 to 2009–10' (14 October 2010) 9
[96] Above n.71 [1]
[97] Above n.69, para.12.4 – 12.5
[98] Per s.64A of the Police and Criminal Evidence Act 1984.
[99] Above n.71 [6]
[100] Above n.68
[101] Ministry of Justice: 'Simple Cautions for Adult Offenders: guidance for police officers and Crown Prosecutors' (13 April 2015) at para.6

a 'simple caution'.[102] There has never been any statutory basis for the administration of simple cautions – they are merely 'a discretionary procedure adopted by the police'[103] which has been *in situ* since at least 1929[104] and very likely much earlier.[105] In theory, a simple caution is a possible disposal for any offence, subject to the statutory restrictions on their use in indictable (and some triable either way) matters.[106] In practice, however, simple cautions 'are primarily intended for low-level, mainly first-time, offending'.[107] Home Office guidance is now routinely produced[108] to assist the police and prosecutors in their use and the present position is that a simple caution must only be given when a suspect makes 'a clear and reliable admission of guilt',[109] where there would be sufficient evidence to prosecute the offender, if required[110] and where either the police or the CPS believe it is in the public interest to issue a simple caution.[111]

'Simple cautions' are now distinguished from 'conditional cautions', which are issued pursuant to a statutory framework[112] which allows for conditions to be attached to a caution with which the offender must comply.[113] There are statutory requirements for the issuing of these, including that a prosecutor is satisfied that there is sufficient evidence to prosecute and that a caution is an appropriate means of disposal[114] and that the offender admits the offence.[115]

A parallel programme exists to caution juveniles. This was initiated in limited form in 1929 and reflected a general principle that 'the straightforward retributive response which is proper in the case of an adult offender is modified to meet the needs of the

---

[102] Ibid
[103] *R v Commissioner of the Police of the Metropolis ex parte Thompson* [1997] 1 WLR 1519 [2] (Schiemann LJ)
[104] *R v Chief Constable of Kent and Another* [1991] 93 Cr. App. R. 416, 421 (Watkins LJ)
[105] In R (on the application of Stratton) and Chief Constable of Thames Valley Police [2013] EWHC 1561 (Admin), the President of the Queen's Bench Division stated that 'the practice many have begun early in the nineteenth century' [21].
[106] Per s.17(2) – (3) of the Criminal Justice and Courts Act 2015.
[107] Ibid, s.17(4)
[108] Above n.100 and Ministry of Justice, 'Code of Practice for Adult Conditional Cautions – Part 3 of the Criminal Justice Act 2003' (January 2013) are the two relevant provisions.
[109] Above n.101, para.20
[110] Ibid, para.24
[111] Ibid, para.26
[112] Created by s.3 of the Criminal Justice Act 2003
[113] Per s.22(2) of the Criminal Justice Act 2003
[114] Per s.23(2) of the Criminal Justice Act 2003
[115] Per s. 23(3) of the Criminal Justice Act 2003

individual child'.[116] Section 5(2) of the Children and Young Persons Act 1969 formally recognised the provision of juvenile cautions and, like adult cautions, these could only be issued if the juvenile freely admitted the offence.[117] Juvenile cautions were outlawed when the FWS was implemented[118] but provision to issue conditional cautions was made in 2008[119] and simple cautions for juveniles replaced the FWS in 2012 .[120]

Cautions are advantageous to the recipient because although the issue of a caution is usually 'a sensitive, certainly embarrassing and probably shameful part of [an individual's] history', they are issued in private and, therefore, like reprimands and warnings, they do not form a matter of public record.[121] Simple cautions 'carry no immediately disagreeable consequences for the offender'[122] and at common law they are not a form of sentence, nor are they a conviction.[123] Unlike reprimands and warnings, which were issued at the discretion of police officers, a caution can only be issued if a suspect consents to it.[124]

In view of the advantages inherent to the caution as compared to a prosecution, many suspects unsurprisingly choose to accept one. This is particularly so as regards juvenile offenders, where a significant proportion of offences have historically been so disposed: by 1993, 90% of boys and 97% of girls were diverted from the court system to police cautioning.[125] In broadly the same period, the cautioning rate among adult offenders was around 11%.[126]

One of the long-standing, principal benefits those cautioned was that, although often recorded on local police force systems,[127] cautions were not formally recorded by any

[116] Above n.71 [24]
[117] J.A.F. Watson and P.M. Austin, *Modern Juvenile Court* (Shaw & Sons Ltd 1975) 80
[118] Per s.67(8) of the Crime and Disorder Act 1998
[119] Per s.48 of the Criminal Justice and Immigration Act 2008, inserting s.66G into the Crime and Disorder Act 1998
[120] Per s.135 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012 which repealed ss.65 – 66 of the Crime and Disorder Act 1998
[121] *R (on the Application of T and another) v Secretary of State for the Home Department and another* [2014] UKSC 35 [17] (Lord Wilson)
[122] Above n.103, 1521
[123] Above n.105 [33]
[124] Recipients do have a genuine choice: if the police offer to caution an individual and that person refuses, then the police must decide to either charge the suspect or release them. See Home Office, 'Circular 30/2005: Cautioning of adult offenders' (14 June 2005), para.19
[125] L. Gelsthorpe and A. Morris, 'Much ado about nothing - a critical comment on key provisions about children in the Crime and Disorder Act 1998' (1999) 11 Child and Family Law Quarterly 209, 210
[126] HC Written Answers 29 March 1993, vol.222, col.101
[127] Home Affairs Committee, *Criminal Records* (HC 285, 1989 – 90, 3) para.22

of the CROs and were not considered part of a 'criminal record'.[128] A Home Affairs Committee reviewing criminal records in 1990 baulked at the notion of disturbing the status quo, describing the central retention of cautions as 'a radical innovation' which was 'not practical'.[129] However, just one year later an Efficiency Scrutiny recommended that, once the criminal records were computerised, all cautions be collated and recorded[130] with the Government soon-after confirming that cautions would henceforth form part of the national collection of criminal records.[131] The police began adding cautions to the PHOENIX database on 1 November 1995.[132]

The decision include cautions in central records has several possible explanations. The first is that computerisation, by negating entirely the practical problems of storing millions of records, opened the theoretical possibility of storing far more criminality data.[133] PNC2, with its vastly improved storage capabilities, made the retention of cautions a practical feasibility, and therefore by extension facilitated it. This had been foreseen by the Data Protection Registrar, whose caution in 1990 that 'the capacity of PNC2 should not become a motivating force for information to become excessive'[134] was not heeded. Moreover, PNC2 was encouraging a move towards 'intelligence-led policing'; a supposed 'proactive' policing strategy based on focusing resources in accordance with reliable intelligence of crime and criminals.[135] It was argued that such an approach could only be taken if the full 'intelligence picture' was available, including instances of trivial offending such as that disposed of by cautions.[136] Finally, at the time that the decision to include cautions was taken, plans were well advanced for bringing legislation which would expand significantly access to criminal records for employment vetting purposes. Those proposals required the retention of cautions.[137]

[128] 'Criminal Justice Bill', H.L Deb, 21 May 1991, vol.529, col.198
[129] Above n.127 at paras.29 – 30
[130] Home Office, 'The National Collection of Criminal Records: report of an efficiency scrutiny' (HMSO 1991), para.48
[131] HC Written Answers 20 July 1993, vol.229
[132] HC Written Answers 6 February 1996, vol.271, col.113
[133] Above n.23, 88 – 90
[134] Above n.127, para.30
[135] Audit Commission, 'Helping with enquiries: tackling crime effectively' (HMSO 1993) 35 – 38. A fuller examination of this is offered in the next chapter.
[136] *Chief Constable of Humberside Police and four others v Information Commissioner* [2009] EWCA Civ 1079 [28]
[137] This is discussed in more detail at ch.8.5 of this research.

Whatever the explanation, the decision to include cautions on PHOENIX meant that the number of individuals who had criminal records grew accordingly: in 1998 alone, some 109,700 juvenile cautions were issued.[138] This accumulation was almost certainly accelerated by the institution in 2000 of central government targets aimed at increasing the volume of offences resulting in an 'offender brought to justice'; defined as when an offence had taken place and the police were able to identify the perpetrator and either issue a caution, reprimand or warning or when the suspect was charged.[139]

It is submitted that these targets effectively forced police officers to deal formally with extremely trivial matters that might ordinarily be dealt with informally; indeed, the Chair of the Youth Justice Board resigned in 2007, bemoaning a 'disastrous' policy which encouraged police to 'pick a lot of low-hanging fruit'.[140] The targets were only removed in 2008 and almost certainly account for the marked decline in cautions issued since: some 362,895 were issued in 2007 as compared to 83,989 in 2017.

That notwithstanding, the number of cautions issued during that period and since remain very substantial: between 2002 and 2017, the police issued approximately 3,688,000 cautions.[141] The precise number of nominal records which include only one caution is not known[142] but it is submitted that there must be hundreds of thousands of such records due to the nature of the circumstances in which cautions are properly administered. It is further submitted that the decision to include cautions in the criminal records, almost always issued in respect of first time, trivial offences, substantially widened the scope of a 'criminal record' and encompassed within it hundreds of thousands of people who would not have been so engaged prior to the computerisation of the national collection.

---

[138] Above n.71 [4]
[139] C. Williams, 'The growth and permanency of Criminal Records, with particular reference to juveniles' (1 June 2011) 84(2) Police Journal 171
[140] R. Morgan, 'What's the Problem?' (2007) 157 New Law Journal 305
[141] Ministry of Justice, 'Criminal Justice Statistics, Quarterly Update to December 2012, England and Wales' (30 May 2013) 23 and Ministry of Justice, 'Criminal Justice Statistics Quarterly, Out of Court Disposals 2007 – 2017, Pivot Analytical Tool for England and Wales' (17 May 2018) Cautions Pivot Table. Figure has been rounded to the nearest thousand.
[142] The Home Office claim that the PNC does not make any distinction between disposal type on PHOENIX, and that it would require a software re-write to do so; see Home Office, 'FOI Request. Number of people with criminal convictions on the PNC' (FOI Reference CR33517, *What Do They Know?* 13 November 2014) <https://www.whatdotheyknow.com/request/number_of_people_with_criminal_c#incoming-595350> accessed 7 August 2018

3.4.4 Penalty Notices for Disorder

Penalty Notice's for Disorder (PNfDs) were created by the Criminal Justice and Police Act 2001 ('the 2001 Act'),[143] which provided that where a constable suspects an individual has committed a specified offence[144] s/he may give him a penalty notice[145] which, upon the payment of a specified fee, will discharge any liability to be convicted for that offence.[146] The individual in question must be over 18 years old[147] and must pay the specified fee within 21 days or risk court proceedings being instigated against them.[148] Commonly referred to as 'on the spot fines',[149] they are intended as 'a quick and effective alternative disposal option for dealing with low level, anti-social and nuisance offenders'[150] – examples of offences which might attract a PNfD include shop-thefts with a value of under £100 (plus VAT)[151] and criminal damage valued at under £300.[152]

PNfDs are different at law to reprimands, warnings and cautions. In interpreting the legislation which governs them, the Court of Appeal explained that: 'the issue of a notice is not a conviction. It is not an admission of guilt nor any proof that a crime has been committed…[a person accepting a PNfD] was not admitting any offence, not admitting any criminality, and would not have any stain imputed to his character'.[153] For these reasons, it is sometimes (erroneously) said that 'a PNfD does not create a criminal record',[154] yet the reality is that the police *do* record PNfDs on PHOENIX (where they relate to a 'recordable offence');[155] a person subject to such a PNfD will have a nominal record created/updated against their particulars and the PNfD is entered into the 'Event History' index.[156]

---

[143] As subsequently amended by s.132 and Schedule 23 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012
[144] These are listed in s.1 of the Criminal Justice and Police Act 2001
[145] Ibid at s.2(1)
[146] Ibid at s.2(4)
[147] Ministry of Justice, 'Penalty Notices for Disorder (PNDs)' (24 June 2014), para.1.10
[148] Above n.144, s.5(1)
[149] This is the most commonly used term, particularly in the news media: see 'Shoplifters to get fine let-off' *BBC* (30 May 2007) <http://news.bbc.co.uk/2/hi/uk_news/6703813.stm> accessed 16 May 2019
[150] Above n.147, para.1.1
[151] Ibid at para.3.13
[152] Ibid at para.3.19
[153] *R v Hamer* [2010] EWCA Crim 2053 [15] (Thomas LJ)
[154] *R v Gore and Another* [2009] ALL ER (D) 139 (Jul) [11] (Lord Chief Justice)
[155] A. Edwards, 'In Practice: Criminal Law – Conditional Cautions' (29 May 2008) Law Society Gazette 19
[156] Above n.6, para.1.1.6

Supporters of PNfDs claim that they free the courts from a cluttering of trivial matters which would consume significant resource and that the (very) public imposition of them act as a deterrent.[157] They also claim that those who are 'wrongly' issued a PNfD have the right to refuse it and challenge the allegation in court.[158] Critics, however, claim that they are a rudimentary form of summary justice, with officials 'sitting as judge and jury, interpreting the law as they see fit'.[159] Indeed, one academic claimed that: 'police officers are giving out PNfDs to people who have not committed any criminal offence…[and] are being given out where the use of some discretion could remove the need to take any formal action at all'.[160]

These criticisms are (at least partially) reinforced by media reports of egregious examples of PNfDs issued for littering to a man who dropped a ten pound note on a pavement[161] and a woman who was feeding ducks.[162] As to the possible recourse of a suspect to the court to challenge a PNfD, critics counter that 'only a handful [of those issued PNfDs go to court, for obvious reasons. Only one percent are actually challenged'.[163]

This lends PNfDs to similar 'net widening' criticism as those raised against warnings, reprimands and cautions; the police have issued 1,535,521 between 2005 and 2017.[164] Precisely how many of these were recorded on PHOENIX is not known, but it is submitted that it must be quite a significant number: between 2005 and 2009 alone, 199,692 PNfDs were issued in respect of shop theft, 325,180 in respect of harassment, alarm or distress while another 215,517 were issued in respect of drunk and disorderly

[157] R. Epstein, 'Summary Justice: fast – but is it fair?' (29 November 2008) 172(48) Justice of the Peace and Local Government Law 791
[158] Above n.153 [13] and also per s.4(2) of the Criminal Justice and Police Act 2001
[159] See R. Appleton, 'Pavement Injustice: the tyranny of on-the-spot fines' (The Manifesto Club 9 February 2012)
[160] K. Reid, 'Is there a problem with PNDs?' (19 October 2013) 177(42) Criminal Law and Justice Weekly 687
[161] M. McGivern, 'Cops hit man with £50 fine – for dropping £10 note in the street' *Daily Record* (Glasgow, 11 June 2009)
[162] L. Finnigan,' Litter Wardens suspended after woman fined £80 for feeding ducks' *The Telegraph* (London, 30 September 2016)
[163] Above n.157
[164] Ministry of Justice, 'Criminal statistics annual report: chapter 2, Penalty notices for disorder' (4 May 2012) and Ministry of Justice, 'Criminal Justice Statistics, Quarterly: Out of Court Disposals Tools (December 2017)' (17 May 2018)

behaviour.[165] Each of these is a 'recordable' offence (see below) and therefore should, and very likely would, have been recorded onto PHOENIX.

3.4.5 Convictions[166]

A conviction is 'a legal, conclusive finding of guilt'.[167] There has never been an attempt to compile a complete register of all convictions in England and Wales. The first criminal record register[168] aimed to collate the names of '*all persons* convicted of a crime' (authors emphasis). It did not require that a register of *all convictions* be kept. After even this limited collection became unusably voluminous, the second register required the registration only of those who had been convicted twice or more of an imprisonable offence.[169]

By 1912, the National CRO was had expanded its collection to any person convicted of any offence which resulted in a sentence of one month imprisonment or more.[170] Although this re-incorporated first-time offenders into the ambit of the collection, the Metropolitan Police continued to delineate between 'serious' and 'minor' offences, where 'serious' was measured by the sentence handed down. The resultant criminal record collection was far smaller than that in other countries.[171] The Metropolitan Police made their decision independent of any legislative amendment or addition to their collection powers; indeed, between 1967 and 1984 there existed no statutory requirement or authority to collect any records yet the police simply continued to compile their record of 'serious' offences.[172] No legal challenge to that decision was ever brought and Parliament willingly deferred entirely to the supposed operational requirements of the police.[173]

Section 27(4) of the Police and Criminal Evidence Act 1984 ('PACE 1984') provided that 'the Secretary of State may by regulations make provision for recording in national

---

[165] Ministry of Justice, 'Criminal statistics annual report: chapter 2, Penalty notices for disorder' (4 May 2012)
[166] Above n.68, section 3(1)(a)
[167] *R v Farinacci* [1993] OJ No 2627 (QL) (Arbour J A)
[168] Per s.5 of the Habitual Offenders Act 1869
[169] Per s.7 – 8 of the Prevention of Crimes Act 1871
[170] C. Matthews, *The Police Code and General Manual of the Criminal Law* (15th edn, Butterworths and Co 1912) 51 – 52
[171] B. Thompson, *The Story of Scotland Yard* (Grayson & Grayson 1925) 201
[172] The Home Office cautioned in 1976 that those relying on criminal record checks should take care as 'not all criminal convictions are recorded' (above n.1, 85).
[173] HC Deb 9 June 1964, vol.698, col.729 – 30

police records convictions for such offences as are specified in the regulations'. In January 1986, the first such regulations mandated that 'recordable offences'[174] be kept. A 'recordable offence' is any offence where the offender 'could incur a prison sentence, whether or not they had'.[175] In addition, four other specified offences were listed as 'recordable'[176] and the police were required to record *all* convictions obtained against an individual who is convicted of multiple offences in the same proceedings.[177]

This legislation appeared to mark a clear re-shift from collecting information relating specifically to *offenders* onto *offending*: the clear intention was to record all relevant convictions, rather than to simply compile a list of offenders. The list of recordable offences was subsequently extended in 1989[178] and 1997, when 43 additions were made.[179] The National Police Records (Recordable Offences) Regulations 2000,[180] attempted to consolidate increasingly disparate provisions by revoking all previous applicable regulations but retaining the basic definition of a 'recordable offence'[181] and the requirement to record multiple convictions where one in the proceedings was recordable.[182]

It also provided an exhaustive list of 52 specified, non-imprisonable but nonetheless 'recordable' offences to be included on PHOENIX. This included such disparate offence as drunkenness in a public place,[183] throwing missiles onto a football pitch,[184] unlawful possession of a police uniform,[185] various public order offences including failure to follow instructions[186] and riding a pedal bicycle without the owner's consent[187] - all of which now fell to be recorded.

---

[174] *R v Chief Constable of B and another ex. Parte. R* [1997] Lexis Citation 4824 (Laws LJ). Thomas (above n.3, 26) notes that the term 'reportable' was widely used at the time, and that 'reportable' and 'recordable' became synonymous. By the 1990's, 'recordable' was the primary term used.
[175] Per the National Police Records (Recordable Offences) Regulations 1985, S.I. 1985/1941 at Reg.2(1) and also above n.3 at 25 – 6
[176] Ibid, Reg.2(1)(a – c)
[177] Ibid, Reg.2(3)
[178] The Police National Records (Recordable Offences) (Amendment) Regulations 1989, S.I. 1989/694
[179] Per Reg.2 of The National Police Records (Recordable Offences) (Amendment) Regulations 1997, S.I. 1997/566
[180] Per Reg.2 of The National Police Records (Recordable Offences) Regulations 2000, S.I. 2000/1139
[181] Ibid, Reg.3(1)
[182] Ibid, Reg.2(3)
[183] Ibid, Schedule of Specified Offences, para. 4
[184] Ibid, Schedule of Specified Offences, para. 12
[185] Ibid, Schedule of Specified Offences, para.30
[186] Ibid, Schedule of Specified Offences, para.37
[187] Ibid, Schedule of Specified Offences, para.52

What was apparent was that Parliament intended to expand the definition of 'recordable offences' to include many offences which are not 'serious'. That must inevitably mean that more individuals fell within the ambit of the PHOENIX collection. Indeed, further amending regulations in 2003,[188] 2005,[189] 2007,[190] 2012[191] and 2016[192] indicates that Parliament is perpetually engaged in increasing the list of specified recordable offences, which in turn will mean that those captured on the PHOENIX collection will continue to grow.

That notwithstanding, it would be a mistake to envisage the PHOENIX record as a largely complete criminal record collection save exceptional omissions. Even with frequent statutory enactments increasing the scope of central record collection, PHOENIX still contains only around half of all court convictions; the remainder are recorded locally on individual police force systems.[193] It is submitted that this is unsatisfactory for a number of reasons. The attempt to consolidate the list of non-imprisonable recordable offences into a single piece of legislation has palpably failed. The current piecemeal approach, which sees incremental additions and removals made by an almost ceaseless implementation of amending legislation, makes it extremely difficult to know what is 'recordable' and what is not. It is, therefore, easy to envisage that very many people will not know whether they have 'a criminal record' until or unless they take steps to determine this. It is submitted that the widening use of criminal records[194] makes such confusion unacceptable.

It is further submitted that the current prescribed list of non-imprisonable but recordable offences is arbitrary and produces absurd results. This research has already highlighted offences which are ordinarily trivial but recordable, yet conversely, there are a number of offences – such as driving without insurance[195] causing unnecessary

[188] National Police Records (Recordable Offences) (Amendment) Regulations 2003, S.I. 2003/2823
[189] National Police Records (Recordable Offences) (Amendment) Regulations 2005, S.I. 2005/3106
[190] National Police Records (Recordable Offences) (Amendment) Regulations 2007, S.I. 2007/2121. These amendments included adding ticket touting at specified football matches to the list of recordable offences.
[191] National Police Records (Recordable Offences) (Amendment) Regulations 2012, S.I. 2012/1712
[192] National Police Records (Recordable Offences) (Amendment) Regulations 2016, S.I. 2016/1006
[193] S. Mason, 'A common sense approach: a review of the criminal record regime in England and Wales (Report of phase two)' (Home Office, 30 November 2011) 17 and also see above n.82
[194] This is the subject of the next chapter of this research
[195] Contrary to section 143 of the Road Traffic Act 1988

suffering to animals[196] and reproducing British currency notes[197] – which are often not trivial at all but nonetheless remain unrecordable.

There are two diametrically opposed potential solutions. The first is that more offences should be designated as recordable. This approach was advocated in 1990 by a Home Affairs Committee[198] and was reiterated during an independent review of the criminal records in 2010, which stated that it was desirable to obtain 'a more complete set of central records to support public protection arrangements'.[199] The natural extension of this argument is that *all* convictions should be recorded. This has been technically possible since the implementation of PNC2 and would bring some obvious advantages. A complete record might further some of the purposes of retaining the record discussed in the next chapter. Furthermore, it would end the need for routine amending legislation of the kind currently produced. It would also end any confusion as to what is recorded and create a simple, 'bright line' position which the public would understand.

Conversely, there are those who believe that there are too many offences now recorded. In 1992, Liberty said that they 'were not convinced' that there was a need to record all offences on the PNC. They were concerned that this would mean a doubling of those who were fingerprinted, with or without consent. Others, including former senior police officers,[200] have bemoaned the recording of trivial offences as counterproductive to reformative and restorative programmes; one commentator responded to the making of begging a recordable offence[201] by claiming that 'we should be encouraging more local partnerships and not using the comparatively inefficient and unsuccessful criminal justice system to deal with problems of this sort'.[202] It is also evident that recording all offences would significantly widen the net of those included on PHOENIX. Such an approach would inevitably result in PHOENIX containing millions of new 'criminal records'.

Despite the incursions made by 'specified' offences, it appears that Parliament accords with the general premise that central records should be, as they have always been,

[196] Contrary to section 4(1) and (2) of the Animal Welfare Act 2006
[197] Contrary to section 18 of the Forgery and Counterfeiting Act 1981.
[198] Above n.127, paras. 29 – 30
[199] Above n.193, 18
[200] Above n.154
[201] Above n.188, Reg.2(5)
[202] A. Turner, 'Respect and Responsibility' (29 March 2003) 167 Justice of the Peace 221

predominantly a record of the most 'serious' offences. This explains their determination that 'recordable' offences broadly equate to 'imprisonable' ones. The problem is that very many offences are theoretically imprisonable, but in practice rarely result in such disposal; for example, any offence under s.1 of the Theft Act 1968 is recordable became it carries a theoretical disposal of up to seven years imprisonment,[203] yet hundreds of thousands of theft cases are trivial – in 2017, there were some 385,000 incidents of shop-theft.[204] It is doubtful that the majority of such offences would be deemed 'serious'. If the Government intends to record 'serious' offences only, it should find a better way to define 'serious'. The present definition, which incorporates offences which might result in the issue of a caution, cannot reasonably be said to do so.

It is, therefore, submitted that the definition of 'recordable offence' should be reconsidered. A position which invites entirely different criticisms from alternate ends of a spectrum appears entirely unsatisfactory. This author suggests that the Government has two choices, and that choosing either is preferable to the present position.

3.5 Conclusions

The CRO system of compiling criminal records imposed practical limitations of what could be collected, stored and maintained. Computerisation was expected to alleviate those limitations, but progress was very slow and seemed to suggest that, despite police and political proclamations to the contrary, the criminal record collection was not quite as important to policing and criminal justice as claimed.

Despite this, the introduction of a faster, larger computer brought an opportunity not just to finally computerise the existing records but ultimately to collect and store far more new records than previously envisaged. The introduction of PNC2 coincided with a series of central government policy decisions which deliberately, and significantly, widened the net of those falling within the ambit of the central collection of criminal records. Some, such as the extension of 'recordable' offences, have attracted support among many in the criminal justice system and are justiciable on several grounds.

[203] Per s.7 of the Theft Act 1968
[204] This figure is for 2017: see Office for National Statistics, 'Crime in England and Wales, year ending December 2017' (28 April 2018) Table 3

Others, however, are less easily defended. The inclusion of those dealt with by caution – a mechanism specifically developed, and operated for centuries, to keep minor and one-off offending out of the central collection of records – added millions of such offenders into the system for the first time, particularly once the government introduced formal police detection targets which encouraged increased issuing of cautions. Likewise, the FWS, which mandated formal police engagement in situations where previously officers had a wide operational discretion to deal informally with low level youth criminality and forced police to centrally record those warned and reprimanded, brought into the scope of centrally collected criminal records millions of children; now formally criminalised in many cases for petty acts which previously would have gone unrecorded. The introduction of PNfDs have seen the creation of central criminal records for individuals who have not been convicted of a crime or even admitted to committing one in circumstances where the very existence of a criminal act has not been evidentially tested in any way.

The immediate impact of these conscious policy decisions was the creation of millions of new nominal listings, often recording very trivial and occasional offending. This marked a clear departure from the prevailing doctrine of almost one hundred and fifty years of criminal record collection, which concentrated on documenting only the most serious and recidivistic offenders so that police might better investigate crime. The almost unavoidably obvious conclusion must be that this expansion occurred for no better reason than that PNC2 allowed it.

So far as the first research question is concerned, what is now evident is that the 'traditional' view of a criminal record being merely a list of court convictions cannot stand. In the literal sense at least, the 'criminal records' have expanded significantly beyond that point. If PHOENIX must now be considered *the* criminal records, then the data contained within it must also surely be considered an individual's 'criminal record'.

4
The contemporary justifications for PHOENIX

4.1 Introduction

As has been shown, the stated purpose(s) for the collation of criminal records is an extremely malleable concept which has been re-posited on numerous occasions. Henry Fielding hoped to use criminal intelligence to inform police work and prevent crime,[1] the first national collections aimed to aid supervision of released convicts[2] while the National CRO hoped to provide a 'clearinghouse'[3] for crime and criminals in the benefit of solving offences reported to them.

There is no express statutory purpose for the modern collection of criminal records on PHOENIX, although the Data Protection Act 2018 does provide obliquely that data retained for 'law enforcement purposes' (which presumably includes criminal records) is used for 'the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to national security'.[4] This is not dissimilar to the purpose provided by police to the Data Registrar in 1995; namely that criminal records are used in 'the prevention and detection of crime: apprehension and prosecution of offenders; protection of life and property; maintenance of law and order, and rendering assistance to the public.'[5]

This type of generic and overly-simplistic exposition paints an unsatisfactory depiction of the modern utilisation of criminal records in England and Wales; in fact, there are now an extraordinarily wide range of circumstances in which the PHOENIX data is used. There is not scope within this research to provide a detailed critical evaluation of each one of these, but, in order to provide an essential context to the analysis of whether the present policy for the collation, storage and retention of data is 'excessive' (per the fourth research question) which follows in subsequent chapters, and also to allow for an evaluation of the justicability of the expansion of the PHOENIX records outlined in the previous chapter, some critical analysis must be provided.

---

[1] J. McMullan, 'Policing reform and moral discourse: the genesis of a modern institution' (1998) 21(1) Policing: An international journal of police strategies and management 158, 159
[2] HC Deb 4 August 1869, Col. 1261 cited in T. Thomas, *Sex Crime, Sex Offending and Society* (Routledge 2015) 44
[3] R.B Fosdick, *European Police Systems* (The Century Co. 1915) 327
[4] Per Pt. 3, Ch.1, s.31 of the Data Protection Act 2018.
[5] Cited in *Roy McGregor v John G McGlennan* 1993 S.C.C.R 852, 854

What follows in this chapter, therefore, is an attempt to identify the principal purposes for which the PHOENIX collection is used and, where appropriate, to offer some critical insight into some of the avenues of challenge which might be raised against that utilisation which necessarily feed into the detailed critical evaluative research offered in chapters seven to nine of this thesis which deal with the fourth research question.

4.2 The 'criminal records help to prevent crime' purpose

The presumption that collecting and retaining a collection of known offenders helps to prevent crime can be traced back to the middle of the 18th century. It is predicated on two universally recognised, correlating statistical observations; firstly, that prior offending is among the most reliable predictors of future offending[6] because, secondly, a disproportionately large volume of crime is committed by a relatively small number of 'prolific', recidivistic offenders. This pattern, surmised by the Fielding brothers at Bow Street,[7] was identified in a semi-systematic manner by Patrick Colquhoun, who in 1806 concluded that 'it is known that many convicts…return to their old courses'.[8] Indeed, it was a fear of the 'habitual offender' that directly resulted in the first national criminal record collections; in 1915, Fosdick found that between 60 and 70 percent of those convicted of crimes in England between 1900 and 1912 had at least one previous conviction. This led him to proclaim that 'the bulk of crime is committed by those who have been previously in the hands of the police'.[9]

The notion that a small number of recidivistic offenders commit disproportionately large numbers of offences continues to permeate crime prevention discourse.[10] The Home Office reported in 2001 that, of an active offending population of around 1 million offenders, some 10% were responsible for more than half of all reported offences.[11] More

[6] M. Redmayne, *Character Evidence in the Criminal Trial* (Oxford University Press 2015) 31
[7] B. S. Godfrey, D. Cox and S. Farrall, *Serious Offenders: a historical study of habitual offenders* (Oxford University Press 2010) 6
[8] P. Colquhorn, *Treatise on the Police of the* Metropolis (7th edn, Patterson Smith Publishing 1806) 99
[9] Above n.3, 316
[10] Audit Commission, 'Helping with Enquiries: Tackling Crime Effectively' (HMSO 1993) 54, para.125
[11] Home Office, 'Criminal Justice: The Way Ahead' (HMSO, 2001)

modern data from the Ministry of Justice shows that there are around 121,000 'persistent offenders'[12] who between them have committed more than 2.7 million convictions.[13]

The very existence of this pattern is accurately observable only through the systematic collection of criminal records. The problem which the police and Home Office have grappled with since this pattern became apparent is precisely how to utilise this knowledge to prevent crime. One possibility is to closely 'supervise' those who are known to be offenders so that they cannot commit further offences. This was the strategy adopted by the Victorians to curb 'habitual' offenders, but supervision is time, cost and labour intensive[14] and could conceivably in modern parlance give rise to serious human rights considerations. The failure of 'ticket of leave' supervision meant that idea that criminal records could be utilised to prevent crime fell thereafter into abeyance in favour of alternative approaches based firstly on police visibility and patrol, then, by the 1970's a 'reactive' approach to crime which focused on *responding* to reported offences, rather than ostensibly attempting to *prevent* them.[15]

This approach did so little to reduce crime levels in areas where it was adopted that one oft-cited analysis witheringly concluded that:

> The police do not prevent crime. This is one of the best-kept secrets of modern life. Experts know it, the police know it but the public does not know it.; Yet the police pretend that they are society's best defence crime. This is a myth. First, repeated analysis has consistently failed to find any connection between the number of police officers and crime rates. Second, the primary strategies adopted by modern police have been show to have little or no effect on crime.[16]

It was the perceived failure of this reactive approach,[17] along with the implementation of the PNC2, which enabled the development of a number of alternative policing models in

[12] This is defined as an individual who has eight or more convictions or other crime disposals registered against them on the PNC. See Ministry of Justice, 'Criminal Justice Statistics quarterly, England and Wales, September 2016 to September 2017' (18 February 2018) 7, fn.14
[13] Ministry of Justice, 'Criminal Justice Statistics quarterly, England and Wales, September 2016 to September 2017' (18 February 2018) 7
[14] This is largely why the Victorians abandoned it: see HC Deb 20 July 1910, vol.19, col 1353
[15] T. Jones, T. Newburn and R. Reiner as cited in A. Liebling, S. Maruna and L. McAra, *The Oxford Handbook of Criminology* (Oxford University Press 2017) 779. 'Reactive' investigation is explored at length in the next section of this chapter.
[16] D. Bailey, *Policing for the Future* (Oxford University Press 1994) 3
[17] Ibid, 780

the early 1990s. Although these are overall now summarised by Reiner et al as consisting largely of 'little more than fancy labels and promotional devices, rather than genuine developments in policing styles and tactics',[18] it was from this period that the notion of 'proactive policing' emerged. Described by Innes as involving 'the prediction and prevention of criminal offending',[19] proactive policing realigned the purpose of police as being those responsible mostly for crime prevention, rather than offender detection.[20] This led to the development of various models for 'trying to determine which individuals and groups are likely to engage in criminality of different kinds',[21] including 'community policing'[22] and, more pertinently so far as criminal records are concerned, 'problem-oriented policing'.

The central premise of 'problem-oriented policing' is that the core of policing should be to deal effectively with underlying police-recurrent problems rather than simply to react to incidents calling for attention one by one as they occur'.[23] The intention to was to make police work more 'analytical', identifying 'patterns' and aiming to solve the underlying cause of these, rather than seeing crime as a 'one-off' discrete event.[24] Methods such as the SARA process and the 'Problem Analysis Triangle' were rolled out in various police forces during the 1990s with varying degrees of success.[25]

In England and Wales, this 'problem oriented approach' was extended into a variant known as 'intelligence-led policing' ('ILP'): a 'nebulous concept'[26] first mooted by the Audit Commission in 1993[27] which broadly intended to prevent crime 'through proactive policing targeted by criminal intelligence' aimed at removing prolific offenders from circulation.[28] Police forces employed specialist data analysts to pore through criminality data[29] and

[18] Ibid
[19] P. Cane and H.M. Kritzer, *The Oxford Handbook of Empirical Legal Research* (Oxford University Press, 2012) 25
[20] P. Joyce, *Criminal Justice: An Introduction* (Routledge, Oxford 2017) 197
[21] Above n.19
[22] Above n.17
[23] K. Bullock and N. Tilley, *Crime Reduction and Problem-Oriented Policing* (Willian Publishing 2003) 1
[24] Above n.15, 781
[25] Ibid and also above n.20, 199
[26] I. Walters, 'The police, young offenders and intelligence-led policing' (2006) 79 4 Police Journal 305
[27] Above n.10, 57, para.129
[28] J. Ratcliffe, *Intelligence-Led Policing* (Routledge 2011) 6
[29] Ibid, 95

provide ‘intelligence’ to specialist groups (or ‘squads’) of detectives who then identified ‘targets’ who were monitored and ultimately arrested, if necessary.[30]

What is evident is that the influence of the IRP and ‘Proactive’ models have been influential in shaping policing doctrine for the last two decades towards ‘an ongoing surveillance of populations at risk and of risk’,[31] that these were widely implemented as policing models in England and Wales between 2000 – 2005, that these were especially directed towards repeat offenders[32] and that these necessitate the collation of ‘vast stores of information’.[33] Indeed, ILP and other forms of proactive, or even ‘predictive’ policing rely on a steady flow of ‘big data’,[34] particularly data relating to offences and offenders.

It is not the intention of this research to determine ‘whether ILP works’. It will suffice instead to say that ILP is not universally regarded as being effective; either as a model for preventing crime or in the way that police officers have implemented it. Advocates of ILP argue that it is based on empirical criminological research and ‘there is some evidence that it is an effective strategy in law enforcement terms’.[35] For example, one study in Minneapolis found that the identification, and subsequent increased police presence in, a ‘crime hotspot’ identified through data analysis resulted in a ‘clear, if modest, general deterrent effect’[36] while Ratcliffe, a strong supporter of ILP as a process and a means of making policing more ‘cost-effective’, highlighted successful identification and specific targeting of repeat offenders as evidence that ILP, properly undertaken, can be effective.[37]

Indeed, ILP was initially lauded as successfully reducing crime rates but criticism began to emerge which claimed that the focus on repetition of offending over seriousness of offence was ‘a deep confusion’,[38] while others argued that the reduction in crime since ILP was introduced was ‘in the main, coincidental’ and that the potential for crime reduction

[30] T. Newburn, T. Williamson and A. Wright, *Handbook of Criminal Investigation* (Willan Publishing 2008) 442 – 3
[31] Above n.19, 26
[32] G. Farrell and K. Pease, *Repeat Victimisation: Crime Prevention Study Series 12* (Monsey, Criminal Justice Press 2001)
[33] Above n.20, 200
[34] This is an almost natural extension of ILP; the notion that statistical predictions of where crime will occur and who will commit it can be made by an analysis of data. See above n.15, 782
[35] M. Rowe, *Introduction to Policing* (Sage Publishing 2014) 252
[36] L. Sherman and D. Weisburd, ‘General Deterrent Effects of Police Patrol in Crime Hotspots: a randomised control trial’ (1995) 12 Justice Quarterly 626
[37] Above n.28, 195 – 201
[38] A. Ashworth, ‘Criminal Justice Act 2003: the sentencing provisions’ (2005) 68(5) Modern Law Review 822, 827

through ILP had been 'widely exaggerated'.[39] In 2003, James published an analysis of the effectiveness of ILP as a means of preventing crime and claimed that there was little evidence that it had actually reduced crime.[40] This position was repeated at length in 2011 by Alach, who outlined all of the perceived problems with ILP and then provided that:

> All of the above criticisms of ILP would be moot if there were clear evidence of the outcome effectiveness of ILP. Unfortunately for supporters of ILP, there is none, and some of its supporters have stated so quite explicitly. In none of the counties which have embraced, or are embracing, ILP, is there an obvious indication that these new policies and procedures have led to improved policing, however that be defined.[41]

What emerges is that there remains no general consensus as to whether the model of ILP is in itself sufficient justification for the collation, storage and lengthy retention of criminal record data for the purpose of preventing crime. What also emerges is that there also exist significant questions as to whether ILP has been actually implemented by police officers 'on the ground'. This is because 'many police departments lack the skill to conduct rigorous evaluation'[42] of the intelligence data and because 'crime mapping creates tension with some of the fundamental cultural beliefs of street-cops that theirs is a craft-based occupation'.[43]

The latter issue has been observed in more than one study; both Gill (in 2000)[44] and Cope (in 2004) provided both qualitative and quantitative analysis[45] of police forces which showed a general mistrust of data analysts by police officers (particularly those who were civilian, rather than police officers). Cope particularly identified a number of weaknesses in the way in which ILP was being 'adopted'; poor data quality,[46] variable quality of analysis

[39] R. Heaton, 'Police resources, demand and the Flanagan Report' (2009) 82(2) Police Journal 95, 100
[40] A. James, 'The advance of intelligence-led policing': the emperor's new clothes'? (2003) 76(1) Police Journal 45
[41] Z. Alach, 'The emperor is still naked: how intelligence-led policing has repackaged common-sense as transcendental truth' (2011) 84(1) Police Journal 75, 88
[42] Above n.28, 189
[43] Above n.31
[44] P. Gill, *Rounding up the Usual Suspects? Developments in Contemporary Law Enforcement Intelligence* (2000)
[45] N. Cope, 'Intelligence-led policing or Policing-led intelligence'? (2004) 44(2) British Journal of Criminology 188
[46] Ibid, 193

produced,[47] poor police training leading to weak understanding of the analysis produced[48] and a police persistence on seeing analysis as simply a means of identifying 'targets' who might lead to arrests[49] were all identified as unrectified issues.

Perhaps more significantly, however, was Cope's analysis that there persisted a general clash of cultures between the police and the analysists which meant that analysis was often simply not acted upon at all; one interviewee told Cope that: 'the biggest frustration of analysts is the fact that people do not action the work that we produce. We're constantly asked about crime levels and what's going on about it but at the end of the day the analysts only produce recommendations. If they're not acted on, there's nothing more that we can do'.[50] As Ratcliffe (correctly) notes; 'this is hardly the model of operation architects of ILP laid out, and is more indicative of a problem of implementation rather than conceptual design'.[51]

That may be so, but it must call into question just how useful data, and particularly criminal record data, is so far as police operational crime prevention practices are concerned. ILP has now been supplemented with various related, but somewhat different initiatives such as the 'Prolific and Other Priority Offender Programme', which involves the co-operative (predominantly with probation and 'Youth Offending Teams') policing of prolific offenders in the hope of preventing reoffending[52] and 'evidence based policing', which involves the hiring by police of professional academic researchers to make policing recommendations based on analysis of the police's own trove of criminality data.[53] More basic examples include simple electronic tagging of known offenders so as to monitor them and undertake 'crime mapping' exercises.[54]

What is clear is that, if policing models based on ILP or 'evidence-based policing' continue to be the preferred model for forces, data will need to be collated, stored and retained so that the 'intelligence' or 'evidence' required can be gleaned. This will include the retention

[47] Ibid, 195
[48] Ibid, 201
[49] Ibid, 194
[50] Ibid, 197
[51] Above n.28, 190
[52] Home Office, 'Prolific and other Priority Offender Programme: five years on: maximising the impact' (HMSO June 2009)
[53] P. Dawson and E. Stanko, 'The best-kept secrets of evidence-based policing' (2016) 16(2) Legal Information Management 64, 65
[54] D. Rose, 'Overview of the week' (2017) 181 Justice of the Peace 192,192 – 93

of criminal records data. However, as the relevance and quality of the data will necessarily impact on the capacity of it to be considered 'intelligence' which might assist officers in the prevention of future offences, it is submitted that the need extends only to provide the criminal record data for 'active' and/or serious offenders, for reasons analysed in greater depth in chapter 8.4 of this research.

4.3 The 'criminal records help to detect offenders' purpose

It is often tritely stated that the collection of criminal records helps to solve crime; indeed, the National CRO referred to the 'catching thieves on paper'.[55] What was meant by this was never expressly provided. Some criminality datasets have measurable utility in linking suspects to offences. The usefulness of fingerprints as a crime detection device, for example, is obvious; indeed, the national computerised fingerprint database, IDENT1, holds (at 31 December 2017) some 8,093,575 records which can be searched against crime-scene prints for precisely this purpose.[56] Likewise, the National DNA Database, which holds DNA samples on 5,374,062 individuals,[57] has obvious crime detecting potential and indeed both 'are used extensively in the criminal justice system in England and Wales'.[58] Custody photographs were uploaded to police systems in April 2014, along with an automated search facility.[59] This collection of around 21 million images (as of January 2018) also has an obvious usefulness in helping police and witnesses to positively identify suspects and others relevant to an investigation,[60] while *modus operandi* data held on the PNC[61] has obvious useful intelligence properties and has underpinned ILP,[62] among other modern policing methodologies.

The usefulness of the PHOENIX list of criminal disposals held against a specified individual in helping to solve crime is, however, far less clear. There are a number of contentions usually raised. The first is that, when faced with a new crime with which s/he is tasked to solve, the diligent police officer will look to the 'criminal record' as part of the

[55] The Metropolitan Police, 'Catching Thieves on Paper: History and Purpose of the Criminal Record Office and the Police Gazette and it's supplements' (MEPO 8/42 1936)
[56] P. Wiles, Annual Report: Commissioner for the retention and use of biometric material, (HMSO March 2018) 7
[57] Home Office, 'National DNA Database statistics, Q4 2017 – 18' (23 May 2018)
[58] Above n.56, 2, para.6
[59] Alastair MacGregor, 'Annual Report: Commissioner for the retention and use of biometric material (HMSO 10 November 2014), para.337
[60] Above n.56, 88, para.306
[61] Home Office, 'The PNC User Manual v.15.02' (December 2015), 10
[62] N. Pope, 'Intelligence led policing or policing led intelligence?' (2004) 44(2) British Journal of Criminology 188, 201

'overall picture' of an offender which, when taken together with the other criminality data outlined above, can help identify the suspect or suspects responsible.[63] This is very vague, and whether such an approach actually produces any quantifiable results is unclear; even the police admit that the usefulness of the record in this context is 'not easy to quantify'.[64] Another justification is that a criminal disposal fixes an individual to a particular location at a particular time. In this context, the actual disposal itself doesn't much matter but the location of the offence, the arrest and the disposal itself, which together place an individual to a particular geographical point at a particular time. It is suggested that this may, therefore, be useful in investigating an unrelated offence.[65] It is not known how often the police use criminal disposal data for this purpose, but it is submitted that, in a time of GPS tracking devices in very many vehicles and every modern mobile telephone being sold, there must surely alternative means of fixing individuals to particular geographical locations[66] as and when required.

The most common justification espoused relates to the 'recidivism' notion; namely that those individuals with criminal records are more likely to commit offences than those who do not. This gave rise to what Moylan described as criminal records being 'a means of enabling new crimes to be traced to old criminals'[67] and the recidivistic behaviour of a significant proportion of those who commit offences continues to play a prominent role in modern criminological[68] and policing practice.[69]

The knowledge that 'criminals…have a general propensity to commit crime'[70] is one thing. The judicious use of that knowledge for crime detection purposes is quite another. The popular image, perpetuated by the media and facilitated by the police themselves, of

---

[63] T. Thomas, *Criminal Records, a database for the criminal justice system and beyond* (Palgrave Macmillan 2007), 63

[64] *Chief Constable of Humberside Police and four others v Information Commissioner* [2009] EWCA Civ 1079 [28]

[65] Ibid

[66] This really is a *very* weak justification in modern England and Wales because there exists an almost limitless number of alternative means of 'linking' an individual to a particular location at a set time. Entry on the electoral role or records held by the Inland Revenue, the Department for Work and Pension or the NHS will routinely tie a person to a particular general area, while monitoring of debit/credit card use or the GPS satellite positioning of mobile devices or motor vehicles can usual provide real-time tracking of individuals with almost complete accuracy. The odds on the police needed a criminal record to place an individual to a particular geographical area where no other means are available must be *extremely* remote indeed.

[67] J.F. Moylan, *Scotland Yard and the Metropolitan Police* (G. P Putnam' Sons Ltd 1929) 188

[68] M. Redmayne, 'The relevance of bad character' [2002] 61 The Cambridge Law Journal 684, 693

[69] K. Soothill *et al*, 'What is the future repeat danger from sexual offenders against children? Implications for policing' (1 March 2005) 37 Police Journal 78

[70] M. Redmayne, 'The relevance of bad character' [2002] 61 The Cambridge Law Journal 684, 968

police detective work ordinarily involves officers arriving at the scene of the crime, closely observing the scene and witnesses, extracting 'clues' before using deductive reasoning and inferential logic to piece together these seemingly disparate 'facts' to solve the case.[71]

The reality is very different. Palmiotto claims that the response to a report of a crime to the police takes three stages. The first involves a 'preliminary investigation' being conducted by a police officer (usually a patrol officer) who receives the report of an offence. The purpose of this is to make a determination as to whether the offence is 'solveable'. To that end, the officer will take statements from any witnesses, secure CCTV, potential forensic evidence and other sources which might show that an offence has taken place and by whom and, most importantly, about who might have committed the offence and where that person (or persons) might now be.[72] Police often refer to 'the golden hour'; this is the period immediately preceding the commission of an offence where the available information which might ultimately allow for the detection of the offender is most readily obtainable.[73] If this 'preliminary investigation' suggests that there is little prospect of 'solving' the case, and particularly if the matter involves a 'minor' offence, then that will often be the end of the matter and no further investigation will take place. Palmiotto claims that very many investigations will end at this point, as the resources required to investigate further are disproportionate to the seriousness of the offence and the likelihood of 'solving the case'.[74]

Conversely, where the initial investigation reveals that either a 'serious' crime has taken place, or that the chances of solving the case are high, then the investigation moves to the next stage; an investigation conducted by either a specialist detective or a team of detectives.[75] This investigation will focus on the identification of possible suspect(s).[76] In many cases, the identification of the suspect will become quickly apparent through an analysis of the material obtained in the preliminary investigation; identification by a witness(es), CCTV footage of a perpetrator, forensic evidence linking an individual to the offence etc. In homicide offences, for example, several studies have shown that the perpetrator is relatively straightforwardly identifiable, and in these cases the police

[71] S. Turnbull, *The TV Crime Drama* (Edinburgh University Press 2014) 25
[72] M. Palmiotto, *Criminal Investigations* (CRC Press 2013) 14 – 15
[73] Above n.20, 121
[74] Above n.72, 17
[75] Above n.35, 200
[76] T. Newburn, T. Williamson and A. Wright, *Handbook of Criminal Investigation* (Willan Publishing 2008) 426

investigation gravitates 'to a significant degree' towards building a prosecuting case against the suspect.[77]

In all of these circumstances it is extremely difficult to envisage what role, if any, criminal records held on PHOENIX plays in the crime detection process. However, far more difficult detective work is where the identification of the suspect is not immediately apparent and the crime is sufficiently serious that an investigation must take place; the 'whodunit' cases.[78] In this case, detectives ordinarily focus initially on those individuals known to the victim, particularly those with the 'means, motive and opportunity' to commit the offence. Innes claims that 'equally important, though, in the police's eyes is whether any of those near the victim have a previous criminal history'.[79] Where this does not yield 'results', once friends and family are eliminated from an enquiry (and the especial focus will primarily fall on those who have previous convictions), the next port of call is to analyse the characteristics of the crime and to try and match this to 'known, local, active offenders' to generate a new pool of suspects.[80] This search of 'suspect populations' will allow for the identification of individuals who are subsequently arrested, detained and interrogated in the hope that they either confess to the offence or reveal useful information which implicates their criminal associates.[81] It is only once these individuals are eliminated from the enquiry that, according to Innes, 'the police will genuinely open up the scope of their inquiries to consider anyone as a possible suspect'.[82]

This approach to identifying suspects, likened to a 'fishing expedition' by several criminologists,[83] is often described as a means of 'suspect centric' crime investigation, focusing resources on known offenders and, when crimes are reported, seeing if these 'fit' information held by police so that a link might be drawn between them.[84] It is in this manner that the repository of criminal records data on PHOENIX might reasonably be presumed to aid in the detection of crime. The introduction of the Queries Using Extended Search Techniques ('QUEST') software onto PHOENIX in July 1998 enabled this approach to

[77] Ibid, 257
[78] Ibid, 263
[79] Ibid
[80] Ibid
[81] Expressly described as such in both T. Newburn, *Handbook of Policing* (Willan Publishing 2008) 435 and also T. John and M. Maguire, 'Criminal intelligence and the National Intelligence Model' in T. Newburn et al, above n.75, 202.
[82] Above n.80
[83] T. Newburn, *Handbook of Policing* (Willan Publishing 2008) 435
[84] Ibid, 441 – 2

proliferate in electronic form, with the promise to officers that 'provided that the information entered into PHOENIX is up to date, QUEST will find who you are looking for'.[85]

By contrast to those detectives using criminal records to help 'identify suspects', many officers appeared to be not using PHOENIX for anything much at all. Indeed, QUEST was intended to alter the perception of many police officers that PHOENIX was little more than 'a record keeping and reference tool'.[86] Whether it did so is open to debate; in 2005, police management were sufficiently concerned that the *Police Journal* was persuaded to run a ten article publicity campaign to highlight the investigative usefulness of QUEST, with one telling officers that they needed to 'wake up to the investigative opportunities they were missing out on'.[87]

What emerges, then, is that very many offences are 'investigated' and investigations closed without any use of the PHOENIX repository at all. Of those investigations which proceed sufficiently to merit a consideration of PHOENIX, a significant number of officers do not appear to use criminal records very much, or even at all, while those who do use them ordinarily do so as a means of investigating offences by effectively 'rounding up the usual suspects'[88] in order to try and identify possible suspects.

It is not the purpose of this research to evaluate the effectiveness of this method of investigation, but some general concluding points might be considered. The first is that it is not clear whether this means of investigating is an effective means of identifying suspects or 'solving' cases. Homicide investigations typically yield very high conviction rates (up to 90%) but this is ordinarily because of the resources attached to then and that most homicides are committed by friends or family of the victim, so the suspect is quickly identified.[89] By contrast, overall it has been said that 'when taken as a whole, most criminal offending is not even investigated'[90] and, even where investigations do take place, the most recent set of Home Office data shows that in 48% of instances the case was closed without a suspect being identified.[91]

---

[85] Ibid, 64
[86] Ibid, 64 – 65
[87] C. Evans, 'Charting Crime' (14 October 2005) Police Review
[88] Above n.78
[89] Above n.76, 272
[90] Above n.35, 194
[91] Home Office, 'Statistical News Release: Crime Outcomes in England and Wales, year ending March 2018' (19 July 2018)

It is also clear that the 'suspect-centric' approach has led to repugnant results. The Police and Criminal Evidence Act 1984 was enacted, at least in part, to rectify the practice of some detectives to respond to reported offence by rounding up 'known offenders' and coercing confessions upon which convictions could be obtained; a practice described by Johns and Maguire 'relatively easy' prior to the implementation of PACE.[92] In some instances, these were obtained through extreme violence; one example in Sheffield involved the use of a rhino whip by a detective to extract confessions.[93] Conversely, the police conviction that crimes are predominantly committed by 'known' offenders has led to investigations where the true perpetrator has evaded capture because the detectives were looking 'in the wrong place'. Instances include the 'Yorkshire Ripper' investigation, where the police mistakenly 'put all their eggs in one basket' and, in doing so, allowed the perpetrator to continue killing.[94]

The net result, it is submitted, is that there must be some considerable doubt as to whether the collation and retention of criminal records can be justified on the basis of their operational useful to the police in crime detection. There appears to be a general *presumption* [authors emphasis] that this data is useful but, except other than in the manner outlined above, it is difficult to see what use these records hold. Morris,[95] for example, claims that the PNC plays 'a vital part' in criminal investigation, but offers no further explanation as to how this is or why he thinks such. Similarly, in an eight-page exposition of 'evidence' which aids police investigations, Joyce notes simply that 'PHOENIX has developed from it's initial role as a record sharing facility to become an investigative tool',[96] but again offers no further explanation as to how this is so.

This is perhaps not surprising. Whilst there is an obvious logic in the requirement to hold criminal record data relating to serious (cases where the police will almost always conduct more than a 'preliminary investigation') or repeat offenders (who might reasonably be considered a suspect in a new offence) there is no obvious reason why old, minor or inactive records might assist in the detection of offences in any way. If this proposition is

[92] T. John and M. Maguire, 'Criminal intelligence and the National Intelligence Model' in T. Newburn et al, above n.75, 202.
[93] Above n.20, 210
[94] Above n.76, 46
[95] B. Morris 'History of Criminal Investigations' in Newburn et al, above n.75, 32
[96] Above n.20, 128

not correct, then there should now perhaps be offered by the police an evidence-based explanation as to how this is so.

The inherent weakness identified here in the argument that the police require the collation, storage and retention of records must be borne in mind as this research progresses to answer the fourth research question in chapters seven, eight and nine of this thesis.

4.4 The 'criminal records help to prosecute offenders' purpose

The criminal justice system presently *in situ* for the prosecution of suspected offenders in England and Wales unquestionably depends upon a record of *some* [author's emphasis] criminal data. A summation of the use of criminal records in this context is that:

> The defendant's record (previous convictions, cautions, reprimands, etc) may be taken into account when the court decides not only on sentence but also, for example, about bail, or when allocating a case for trial.'[97]

This summation hugely understates the perceived importance, and practical utilisation of, criminal records in the prosecution process: the reality is that the PHOENIX collection of criminal records permeate the entire prosecution process. A concise examination and where, how and why these are used is as follows:

4.4.1 Pre-trial disclosure and bail applications

The initial decision on whether to charge a suspect will be taken by the Crown Prosecution Service ('the CPS') after a review of 'all formal disposals' held against a suspect on PHOENIX.[98] To facilitate this (and the other uses outlined below), the CPS have access to 'read only' access to PHOENIX and some other PNC data.[99]

Once a suspect is charged, PHOENIX plays an integral part of the decision-making process regarding bail. The police[100] and the courts[101] have the authority to refuse bail if one of the statutory grounds are made out. The custody officer who makes the police

[97] Part 8A.1 of the Criminal Practice Directions [2015] EWCA Crim 1567
[98] S. Mason 'A common sense approach – A review of the criminal records regime in England and Wales (Report on Phase 2)' (Home Office 30 November 2011) 13.
[99] Above n.61, appendix 8
[100] Section 38(1)(a) of the Police and Criminal Evidence Act 1984.
[101] Schedule 1, part 1, paragraph 2 of the Bail Act 1976.

bail decision will have access to PHOENIX and will very likely take that record into consideration when making a bail determination because the 'antecedent history'[102] of the accused is a statutory factor which must be considered if it 'appears to be relevant' to the bail decision.[103]

Although the magistrates are entitled to ask for a copy of the defendant's antecedents (and the CPS will usually have these to hand),[104] antecedents will ordinarily be introduced as part of a CPS submission that bail should be refused because the accused may commit further offences. This will often be 'substantiated' by reference to the PHOENIX record, which may show that the defendant has a history of committing many other (often unrelated) offences, the same (or similar) types of offence as that with which he has been charged[105] or if the reason for the defendant's offending is ongoing or if the defendant has previously committed offences whilst on bail.[106] As the decision regarding bail is essentially one of whether the defendant can be trusted to answer to bail if granted,[107] it may also be relevant if PHOENIX shows any prior disposals relating to dishonesty offences or if the defendant has previously absconded when granted bail. PHOENIX will also be consulted to see if the defendant is subject to any current/outstanding court orders (community orders, suspended sentence etc). In any of these situations, the CPS will argue that the defendant cannot be trusted sufficiently to be bailed.

The current statutory provisions on bail certainly require that a collection of criminal records be retained, but the reality is that many of the submissions made in bail hearings regarding antecedents are largely reiterations of those which justify the collection of records for crime detection and prevention; in essence, they offer variations of the argument that 'X should not be bailed because X is a recidivist'. Even if this argument is accepted, and antecedents do play a legitimate role in making a bail decision, then it is submitted that this still does not provide a conclusive justification for

[102] The modern 'antecedent history' takes a very similar form to that provided by the National CRO and observed by Rule in 1970, though in essence it 'is a reference to the defendant's previous convictions' (see D. Sharpley, *Criminal Litigation, Practice and Procedure 2017/18* (College of Law Publishing 2017) 137

[103] Schedule 1, part 1, paragraph 9(b) of the Bail Act 1976.

[104] Code for Crown Prosecutors, 'Bail: Opposing Bail, Information for Prosecutors' (7th edn, Crown Prosecution Service 2013)

[105] D. Sharpley, *Criminal Litigation, Practice and Procedure 2017/18* (College of Law Publishing 2017) 138.

[106] Ibid

[107] J. Sprack, *Emmins Guide to Criminal Procedure* (9th edn, OUP 2002) 88

retaining all convictions, regardless of how minor or aged they may be. A single aged conviction for absconding from bail may well be relevant. A single aged caution for shop theft will rarely, if ever, be so.

The use of criminal record data permeates both pre-trial and trial processes. The CPS must include a copy of the defendant's criminal record[108] as part of the 'initial details of the prosecution case' disclosed prior to the first court hearing in a criminal prosecution.[109] The CPS have a statutory obligation to disclose to the defence any material which might undermine the CPS case or assist the defence.[110] This is taken by the CPS to include the criminal record of any prosecution witness, including the complainant, where that might give rise to a defence that the offence was committed by someone else (including possibly the witness[111]) or where the conviction(s) go to the credibility of the witness. As with bail, particular focus will fall on prior disposals involving dishonesty or those specific to the issue of witness credibility, such as perverting the course of justice.[112]

4.4.2 The use of PHOENIX data as 'bad character evidence'

While it was not uncommon for advocates to 'accidently' leave in view a list of the defendants prior convictions on their desks while conducting trials,[113] the general rule historically was that previous disposals should not be revealed to the court during trial so as to not prejudice the presumed innocence of the defendant.[114] That is no longer the case, and immediately prior to trial, an application may be made to adduce evidence of 'bad character' under the various provisions of the Criminal Justice Act 2003 ('the CJA 2003').[115]

It is not the purpose of this research to conduct a critical analysis of the 'bad character' provisions of the CJA 2003. What follows is an abridged summary of the development of the use of bad character provisions so as to provide an insight as to how the

[108] Per r.8.3(a)(ii) and r.8.3(b)(iv) of the Criminal Procedure Rules 2015
[109] Ibid, r.8.2
[110] Per s.3(1)(a) of the Criminal Procedure and Investigations Act 1996
[111] This occurred in *R v Vasilou* [2000] Crim. L.R. 845
[112] See Code for Crown Prosecutors, 'Disclosure of previous convictions of prosecution witnesses' (Crown Prosecution Service 2013)
[113] *The Magistrate*, (July 1986) 47(2), 107
[114] The so-called 'golden thread of English Criminal Law' in *Woolmington v DPP* [1935] AC 462, 481 (Viscount Sankey)
[115] More specifically, see ss.98, 101 and 112 of the Criminal Justice Act 2003.

PHOENIX repository of criminal record data (or at least something comparable to it) is considered 'necessary' to allow for their operation. An (intentionally) brief overview of the arguments in favour of, and against, bad character evidence is offered, again for the purposes of highlighting to the reader the impact that potential future developments might have on the PHOENIX repository.

Although an application to adduce bad character evidence may be made by the defence as regards a prosecution witness,[116] it ordinarily involves the CPS adducing 'evidence of, or a disposition towards, misconduct',[117] where 'misconduct' is 'the commission of an offence or other reprehensible behaviour'.[118] Such evidence 'cannot of itself prove guilt. The prosecution must adduce other evidence to substantiate their case before the jury or magistrates are permitted to take [the defendant's] bad character into account'.[119]

Evidence of bad character can only be adduced if one or more of the seven 'gateways' provided for by s.101 of the CJA 2003 are made out. These include where the bad character evidence may indicate that the defendant has a 'propensity' to commit offences of the kind s/he is standing trial for or where the defendant is alleged to have a propensity to be untruthful.[120] This quite evidently involves adducing records held on PHOENIX. Single prior convictions are less likely to establish 'propensity' than lengthier records;[121] one obvious implication for prosecutors is that they have a vested interest in disclosing as many previous convictions held on PHOENIX against a defendant as permissible, in the hope of establishing the admissibility of them. For this reason alone, the CPS will argue that a complete record of all criminal disposals is necessary.

It is not merely convictions which might be adduced as bad character evidence. Although PNDs are inadmissible as evidence of bad character,[122] there is a presumption that cautions are generally admissible as bad character evidence,[123]

[116] Per s.100 of the Criminal Justice Act 2003
[117] Section 98 of the Criminal Justice Act 2003.
[118] Section 112 of the Criminal Justice Act 2003.
[119] Above n.105, 403
[120] Section 103(1) of the Criminal Justice Act 2003. As with a bail application, these usually involve adducing convictions related to dishonesty offences; see *R v Edwards* [2006] 1 Cr App R 31, 48
[121] *R v Fouad Bennabou* [2012] EWCA Crim 3088
[122] *R v Hamer* [2011] 1 WLR 528 [16 – 17]
[123] *R v Minnis (Martyn David)* [2012] EWCA Crim 461 [10] and G. Branston, 'A reprehensible use of cautions as bad character evidence'? (2015) 8 Criminal Law Review 594

reprimands have been adduced to show both propensity and a lack of credibility[124] and acquittals have been adduced as evidence of bad character, particularly as regards propensity.[125] Where an arrest results in a 'no further action' disposal and the CPS have written to the accused to tell him that the matter is closed in perpetuity, the PHOENIX 'event history' record of it can nonetheless be used as evidence of bad character.[126] The CPS are even entitled to elect not to charge a suspect with the tactical intention of instead using the arrest information as bad character propensity evidence in respect of a different offence.[127]

The provisions of the CJA 2003 mostly work against the defendant, but there are occasions where a defendant will ask that the judge make a direction as to his/her 'good character'. This has historically meant that where a defendant has no previous convictions on their criminal record, the judge would direct a jury that the defendant is more credible and less likely to have a propensity to commit the alleged offence than a person of bad character.[128] The modern position is different. Once a judge has permitted non-conviction, bad character evidence to be admissible, to give a good character direction 'makes no sense'[129] and the judge is obliged to give a bad character direction, even if the defendant has no prior convictions.[130]

Good character, therefore, now means 'far more than having no previous convictions'.[131] Only where a person has no previous convictions and no other alleged, admitted or proven 'reprehensible conduct' is s/he is entitled to be considered of 'absolute good conduct' and receive the benefit of a 'full' good character direction.[132] If the record shows old, minor and irrelevant disposals, the judge has a discretion to direct s/he is of 'effective good character'[133] and therefore receive a full good character direction.[134]

---

[124] *R v Worrel* [2012] EWCA Crim 2657 [10]
[125] These were permitted even prior to the provisions of the CJA 2003 as 'similar fact evidence': see *R v Z* [2000] 3 ALL ER 385
[126] *The Queen v David Reginald Smith* [2005] EWCA Crim 3244
[127] *R v Ngyuen* [2008] EWCA Crim 585
[128] *R v Bryant* [1978] 2 ALL ER 689, 696
[129] *R v Hunter and others* [2016] ALL ER 1021 [72]
[130] Ibid [83]
[131] Ibid [74]
[132] Ibid [77]
[133] Ibid [79]
[134] Ibid [80]

The CJA 2003 provisions have been controversial since their inception[135] and it perhaps worth reiterating that it not within the scope of this research to evaluate at length their merits, or otherwise. However, some general comments might be made. The question of what constitutes 'bad character evidence' and when it is of 'probative' value or 'relevant as to credibility' is very subjective and the decisions are usually made firstly by counsel (who have the first decision on whether to raise the issue or not) and then by the judge (who then decides whether to allow an application and how to direct the jury as to the 'value' of the evidence). Extreme subjectivity usually gives rise to inconsistency, as evidenced by the *extremely* [authors emphasis] lengthy line of case authority generated by the CJA 2003 provisions. Additionally, the admissibility of bad character evidence can significantly delay trials and confuse juries; one case saw three months of a trial taken up by an examination of witnesses and others relevant only to supposed bad character of the defendant.[136]

Moreover, the very admissibility of bad character evidence remains a controversial subject. There is a suspicion among some that the CJA 2003 was introduced by politicians for largely political purposes; the prime minister claimed the CJA 2003 was: 'designed to make it clear that we're not going to have people playing the system and getting away with criminal offences that cause real misery'.[137] Quite what was meant by 'playing the system' was never clarified but what is clear was the intention to facilitate more jury convictions, or, more specifically, to convict defendants who would not be convicted on the strength of the case at hand alone.

While this approach (unsurprisingly) attracted the support of the police,[138] and some practitioners[139] it also attracted significant criticism. A Law Commission report into the extant law of bad character evidence published in 2001 advocated a far lesser reform than that ultimately pursued. The Commission were concerned that bad character evidence unduly prejudiced mock jurors,[140] particularly where the offences disclosed were sexual (especially against children),[141] and that there was little evidence that a

[135] As a starting point on some of the issues at hand, consider J.R. Spencer, 'Evidence of bad character – where are we today?' (2014) Archbold Review 6
[136] *R v O'Dowd* [2009] 2 Cr App R 16
[137] 'Juries learn sex offenders' past' *The BBC* (London, 25 October 2004)
[138] C. Dyer, 'Juries may be told of previous convictions' *The Guardian* (London, 26 October 2004)
[139] Above n.68
[140] Law Commission, *Evidence of Bad Character in Criminal Proceedings* (Law Com No 273, 2001)
[141] Ibid, para.A.24

dishonesty offence meant an individual was generally untrustworthy'.[142] The Bar Council were concerned that the extension of bad character admissibility would (once more) encourage the police to 'round up the usual suspects', rather than conduct thorough investigations.[143] Liberty went further, claiming that the provisions compromised the right to a fair trial, because previous convictions show only that 'they are the type of person more likely to commit such offences, not that they are the person who committed this offence'.[144]

The PHOENIX collection makes the admissibility of 'character' ('bad' and 'good') evidence possible, and while the admissibility provisions exist in anything like their current legislative form, a record of criminal disposal information is essential. It does not, however, follow that a *complete* record be retained, because the development of the law relating to bad character indicates clearly that old, minor and irrelevant offences are not necessarily admissible, nor even likely to be so. This is especially likely to be so when dealing with juvenile disposals or out-of-court disposals.

This research does not seek to determine whether such evidence should be admitted, but the author will rather submit that character admissibility evidence is relatively new, rather subjective, potentially prejudicial and there remains some fervent opposition to its use. If this is a principal justification for retaining the PHOENIX data, then it is submitted that it is a controversial one.

4.4.3 Sentencing offenders

If a defendant pleads guilty, or is found guilty after a trial, the court will move to sentence the defendant. Once the determination of guilt is made, the defendant's antecedent history is 'unlocked'[145] and the Crown will provide a full list of antecedents for consideration by the court as part of the decision on sentencing. This long-standing practice[146] currently involves the provision of personal details and a PHOENIX printout

[142] Ibid, para.6.14
[143] J. Rozenberg, 'Juries will be told of previous convictions' *The Telegraph* (London, 26 October 2004)
[144] 'Liberty's response to the Home Office White Paper 'Justice for All' (Liberty October 2000), para.4.5.1
[145] In *R (on the application of Murchison) v Southend Magistrates Court* [2006] EWHC 569 (Admin), it was held that the critical moment is when the determination on guilt is made, rather than the announcement of the verdict.
[146] Specific practice directions relating the provision of antecedents for sentencing purposes have been issued for decades; see, for example, *Practice Direction (Criminal Law: Previous Convictions)* [1955] 1 ALL ER 386 and also *Practice Directions (Criminal Law: Practice: Particulars of Previous Convictions)* [1966] 2 ALL ER 929

of all recorded prior convictions and cautions. If there are cautions and convictions held on local police force systems, rather than PHOENIX, these should also be provided using the prescribed forms.[147] Where the defendant is to be sentenced in the Crown Court, the police should also provide 'brief details of the circumstances of the last three similar convictions and/or convictions likely to be of interest to the court'.[148] Where the new conviction(s) impacts upon an outstanding court order, such as a suspended sentence, community order or conditional discharge, details of the order should also be provided.[149]

PHOENIX records of past convictions have long played an important role in sentencing. The Crown will adduce previous convictions into evidence during sentencing either with the aim of persuading the court that an offender is dangerous and so the public need protecting from him/her, or that particular types of disposals are (in)effective and should be (re)considered or that the defendant has become a 'persistent' offender or conversely has shown evidence of remorse or rehabilitation.[150] The traditional legal position was that a first-time offender would be sentenced on the basis of being of prior 'good character' and that every subsequent conviction on their record resulted in a progressive loss of mitigation, which would be reflected in sentences of increasing severity on each new conviction.[151]

PHOENIX records of past convictions[152] have, however, assumed a greater importance in sentencing since s.143(2) of the CJA 2003 effectively made them a statutory aggravating factor. This is justified on the basis that an offender is more culpable, and the offence more serious, if an offender has prior convictions: the so-called 'retributive' or 'just deserts' theory of sentencing.[153] It is often stated simply that the provisions of s.143(2) force courts to 'treat each previous conviction as an aggravating factor'[154] and

[147] Above n.97, rule.8A.2
[148] Ibid, rule.8A.6
[149] Ibid, rule.8A.7
[150] Crown Prosecution Service, 'Code for Crown Prosecutors: Sentencing – evidence of character and antecedents: previous convictions' (Crown Prosecution Service 2017)
[151] *R v Queen* (1981) 3 Cr.App.R (S.) 245
[152] The Criminal Justice Act 2003 specifically states 'convictions', which presumably means that cautions are not statutory aggravating factors. They will still be mentioned, though, and may be aggravating, but the discretion lies with the court.
[153] P. Flaherty, 'Sentencing the recidivist: reconciling harsher treatment for repeat offenders with modern retributivist theory' (2008) 8(4) Contemporary Issues in Law 319, 321
[154] J. Roberts, 'Sentencing guidelines and judicial discretion' (2011) 51(6) British Journal of Criminology 997, 1004

indeed this has been treated as a definitive justification for the retention of the PHOENIX collection[155] but the statute does not provide that *all* previous convictions are aggravating. Rather, there are two factors which will determine whether the prior convictions are so: whether the previous offence is 'relevant' to the current offence[156] and whether the previous convictions are recent to the new conviction.[157]

The practical reality is that there will be a subjective judicial assessment of whether a conviction is 'relevant' or sufficiently 'recent' to be considered an aggravating factor. This is in keeping with the subjective nature of sentencing generally, which has become more prescriptive since the introduction of sentencing guidelines in 2003 but which still often turns on whether the decision maker is 'soft' or 'tough' as compared to their peers.[158] Some previous convictions will be considered by some judges to be too old to be relevant to the instant case, some convictions will dispose of offences which bear no resemblance to the present one, some will actually go some way to explain the current offence (and may therefore mitigate it) while in some cases a lack of prior convictions will act as no mitigation because a 'clean record' is almost a pre-requisite for involvement in the offence (offences in respect of drug trafficking, for example).[159]

The impact of prior convictions on sentencing is very widely researched and largely outwith the scope of this research, but some general points may be made. The scope of prior convictions on sentencing is enormous; one study in 2005 found that over three quarters of summary offenders and 88% of those convicted of an indictable offence had previous convictions.[160] Despite regular media and public criticism for perceived leniency in sentencing, particularly the most recidivistic offenders[161], since the introduction of s.143(2) of the CJA 2003, there has been a marked upward recent trend in punitive disposals, record prison populations and concurrent concerns regarding 'sentence inflation'.[162] Indeed, the s.143(2) provisions and the existence of previous convictions can transform a trivial offence into a potentially imprisonable one.

[155] Above n.64 [109]
[156] Per s.143(2)(a) of the Criminal Justice Act 2003
[157] Per s.143(2)(b) of the Criminal Justice Act 2003
[158] R. Epstein, 'The Sentencing Council: what is it for'? (2017) 181 Justice of the Peace 167
[159] J. Rozenberg, 'Columnist: matters of discretion' (2008) 10 Law Society Gazette 18
[160] J.V. Roberts, 'Punishing Persistence' (2008) 48(4) British Journal of Criminology 468, 468 – 69
[161] G. Robson, 'The art of sentencing' (2009) 173 Justice of the Peace 453
[162] Above n.158, 168

In *R v Nourine*,[163] a man who stole a smartphone from a woman in a department store was initially sentenced to two years imprisonment, despite being apprehended at the scene and making a guilty plea, largely because he had 18 previous convictions for similar offences.[164] The sentence was reduced on appeal to 'only' 42 weeks imprisonment.[165] Similarly, in *R v Evans*[166] a man stole £230 from a bookmaker's till in an opportunistic theft and then pushed a staff member while affecting an escape.[167] He was given a twenty-seven month prison sentence after the judge treated 25 previous convictions, mostly for dishonesty offences, as aggravating factors.[168] The Court of Appeal, recognising the difficulty in striking a balance between what the sentencing guidelines indicate for the offences looked at in isolation and a suitable punishment to the particular offender'[169] decided that the trial judge had given excessive weight to the prior convictions but nonetheless sentenced the defendant instead to eighteen months.[170]

Such use of previous convictions in sentencing is unlikely to garner much sympathy for the offender affected by it. The public generally are in favour of the 'recidivistic premium' and studies have shown that they view previous convictions to be the most important factor in determining sentence, other than the seriousness of the crime itself.[171] A majority of victims of crime take a similar view.[172]

It is submitted, however, that there exists legitimate questions to be asked as to whether the views of the public and victims should be the prevailing voices in sentencing offenders, or whether old, minor or irrelevant convictions have any real merit in sentencing offenders or, ultimately, whether a system which effectively transforms otherwise relatively trivial offences into imprisonable ones truly accords with notions of 'fairness' or 'justice'.

[163] [2013] EWCA Crim 73
[164] Ibid [3]
[165] Ibid [13]
[166] [2016] EWCA Crim 31
[167] Ibid [2 – 3]
[168] Ibid [4]
[169] Ibid [11]
[170] Ibid
[171] Above n.160, 472
[172] I. Edwards, 'Sentencing Councils and Victims' (2012) 75(3) Modern Law Review 324, 343

4.5 The (multitude) miscellaneous uses of criminal records

When the PNC was originally mooted, politicians, wary of civil liberty and privacy concerns, were in earnest to reassure the public that access to the system would be strictly limited to only specifically trained and authorised police officers and officials. By 1992 the position has shifted slightly, so that the Home Office, the DVLA and HM Customs and Excise had 'read only' access,[173] but there remained a hesitancy to extend access to the database. The position in 2018 is very different and the PNC is now routinely accessed by police and non-police organisations. Indirect access is available through the ACRO Criminal Records Office ('ACRO'), whose website advises that any organisation who wishes for them to become 'your PNC services provider' should email them 'to discuss products and pricing plans available'.[174] In 2016 – 17, ACRO provided PNC services to 34 non-policing agencies, including the RSPCA, the Maritime and Coastguard Agency and the Gambling Commission.[175]

Direct access to the PNC for non-police organisations is determined by the 'PNC Information Access Panel' ('the PIAP'), constituted by members from the National Police Chief's Council, the Association of Police Authorities and the Home Office. Very little public information relating to the PIAP, or to those organisations whom the PIAP have authorised to access the PNC, exists, though a Parliamentary response by the Home Office in 2009 indicated that the role of the PIAP involved determining whether: a) 'a lawful and justifiable reason for the granting of access' existed; b) what access should be granted for that purpose; and c) ensuring those granted access were able to comply with data protection legislation, keep the data secure and provide suitable training for those with access.

Those who have access are subjected to audit from HM Inspectorate of Constabulary.[176] A Home Office missive lists some 31 non-police agencies with direct access to the PNC.[177] A later request in 2011 saw the Home Office list 18 police organisations with 'full access' (the capacity to read and amend records) and a further 32 agencies granted 'partial access' (the capacity to read the 'names file' on the PNC) by the PIAP.

---

[173] HC Written Answers 15 October 1992, vol.177, col.719
[174] ACRO Criminal Record Office website, 'Police National Computer Services: Requesting PNC services for your organisation' <https://www.acro.police.uk/acro_std.aspx?id=197> accessed 21 August 2018
[175] ACRO Criminal Records Office, 'Annual Report 2016 – 2017' (ACRO 2017) 18
[176] HC Deb 10 March 2009, vol.489, col.305WA
[177] Ibid

This is still an incomplete list – the minister lists only some of the 'other' organisations granted 'partial access' outwith the PIAP process, such as the Royal Air Force police, the Probation Service and HM Courts Service[178] – yet it is perhaps the closest to a publicly available 'complete'[179] list available. Thomas told a House of Lords committee in 2007 that 'no definitive list [of agencies with direct access] appears to exist'[180] while a Freedom of Information request to the Home Office in 2015[181] resulted in the disclosure of a partial list of agencies accompanied by a terse caution that: 'the list provided is not exhaustive. Other cross-governmental departments and agencies have access but we will neither confirm nor deny the names of those departments'.[182]

It is therefore, not possible to provide a definitive list of those who have access to PHOENIX and for what purpose. It is, however, possible to identify some of those with access and to identify what the data is used for. Some of the most pertinent examples are offered below:

4.5.1 The ACRO Criminal Records Office ('ACRO')

ACRO was formed in 2006 to 'help organise the management of criminal record information and improve the links between criminal records and biometric information'.[183] Initially little more than four staff working from 'a temporary accommodation in a police car park',[184] ACRO now employs over 300 staff[185] at its offices at Hampshire Police headquarters and is the unofficial successor to the now defunct NIS.

ACRO, unsurprisingly, has 'full access' to PHOENIX and use it for a multitude of purposes. PHOENIX data is used to compile 'Police Certificates'. These certify whether

[178] HL Deb 21 November 2011, col.205W
[179] The list is now nine years out of date and is clearly no longer accurate; for example, it lists both the Criminal Records Bureau and the Independent Police Complaints Commission, both of which are now defunct.
[180] Memorandum by Dr. T. Thomas' (May 2007) [9] for the Constitution Committee, *Surveillance: Citizens and the State* (HL 2008 – 09, 18–I)
[181] Home Office, 'FOI Request. Agencies with PNC access' (FOI Ref 37592, *What Do They Know?* 22 November 2015) <https://www.whatdotheyknow.com/request/agencies_with_pnc_access#incoming-753180> accessed 16 May 2019
[182] Ibid
[183] Association of Chief Police Officers, 'ACPO Criminal Records Office, Annual Report 2011 – 12' (ACPO 2012) 4
[184] Ibid
[185] Above n.175, 4

a named individual has any 'criminal history' on PHOENIX, and, if so, what.[186] These are issued to help individuals apply for a visa to enter certain countries (e.g. the USA, Australia, New Zealand) where the production of a 'Police Certificate' is a mandatory part of the screening process.[187] PHOENIX data is also used to produce 'International Child Protection Certificates', which reveal whether a named individual has a 'relevant criminal history' when s/he intends to work with children outside the UK.[188] Over 11,000 such certificates were issued in 2016 – 17.[189]

ACRO are also responsible for managing the UK's responsibilities in the international exchange of criminal records. In 2008, the EU laid down a Framework Decision[190] which effectively imposed upon EU member states a legal obligation to ensure that EU citizens accused of crimes be treated the same as national citizens so far as criminal proceedings in each member state are concerned.[191] It is submitted that this must impose a concurrent obligation on members states to retain, and provide access to, national criminality data. Equality of treatment is impossible if the necessary data is unavailable. Measures to ensure compliance with the framework were required to be in place by 15 August 2010.[192] So far as the UK was concerned, PHOENIX was sufficient to ensure compliance.

The European Criminal Record Information System ('ECRIS'), which went 'live' in April 2012, allows for the sharing of PHOENIX data with all but three EU member states.[193] Requests for information from PHOENIX by EU member states, and for criminal record data held by EU states requested by UK police forces and other agencies, are managed by ACRO.[194] It is not clear how this process will be affected by the UK's cessation from the European Union, though it is generally presumed that a mutual cooperation

[186] Her Majesty's Inspectorate of Constabularies, 'Police National Computer Compliance Report', 5 – 7 October 2010 (HMIC January 2011) 5
[187] Ibid, 22
[188] Her Majesty's Inspectorate of Constabularies, 'Use of the Police National Computer: An inspection of the ACRO Criminal Records Office' (HMIC April 2017) 16
[189] Above n.175, 20
[190] Council Framework Decision 2008/675/JHA, July 24 2008
[191] Ibid, Art. 3.1
[192] Ibid, Art. 5.1
[193] European Scrutiny Committee, *EU Afghanistan Cooperation Agreement on Partnership and Development* (HC 2015 – 16, 24-I) [10.1]
[194] Above n.175, 15

arrangement will be sought to allow this data transfer to continue.[195] Plans are also now well advanced to improve the sharing of criminal records of non-EU nationals; an EU Proposal for a Regulation was issued in June 2017[196] to which the UK opted in on 23 October 2017.[197]

ACRO add details of prosecutions brought by agencies who only have 'partial' access to the PHOENIX database, such as the RSPCA, the Environment Agency and the Prison Service. In 2016 – 17, 1,259 records detailing 3,427 convictions were added.[198] They also deal with all subject-access requests relating to the PNC and PHOENIX, manages requests to delete data from PHOENIX and convert historic microfiche criminal records where the offender again 'comes to notice'.[199] In 2016 – 17, over 165,000 subject access requests were received[200] and some 5,402 microfiche records were converted to the PNC.[201]

4.5.2 HM Prison and Probation Service[202]

Before an offender is sentenced, HM Prisons and Probation Service may be asked to provide a 'pre-sentence report' to inform the sentencing decision and staff are provided with 'read only' access to PHOENIX for that purpose.[203] A report is mandatory where the court is considering either a custodial sentence[204] or community order[205] and otherwise a discretionary part of the magistrates court process.[206] The report, which may be in writing or delivered orally,[207] is intended to assist in determining the most suitable method of dealing with an offender[208] and will include reference to the defendant's previous convictions, which are used to help determine the seriousness of

[195] See A. Jackson and G. Davies, 'Making the case for ECRIS: Post-'Brexit' sharing of criminal records information between the European Union and United Kingdom' (1 October 2017) 21(4) The International Journal of Evidence and Proof 330
[196] European Commission, Proposal for a Regulation of the European Parliament and the Council (COD, 2017/0444)
[197] Home Office, 'Impact Assessment: Third Country Nationals and the European Criminal Records Information System' (10 August 2018) 3
[198] Above n.175, 16
[199] Ibid, 17
[200] Ibid, 20
[201] Ibid, 18
[202] Now a part-privatised organisation whose recent work has been strongly criticised. For a thorough examination of the issues, see V. Cowan, 'Probation on trial' (2018) 182 Justice of the Peace 176
[203] HL Deb 21 November 2011, c.205W – 206W
[204] Per s.156(3)(a) of the Criminal Justice Act 2003
[205] Per s.156(3)(b) of the Criminal Justice Act 2003
[206] The starting point is that one will not be required. See above n.97, Part 3A, paras.8 – 9
[207] Per ss.158(1A)(1B) of the Criminal Justice Act 2003
[208] Per s.158(1)(a) of the Criminal Justice Act 2003

the offence and the risk of future offences posed by the defendant.[209] Once more, this sees criminal convictions used in accordance with the 'recidivistic' argument, and the same criticisms raised previously apply once more.

Prison staff are entitled to access to a prisoner's previous convictions when they are newly sentenced or remanded, or when they are being considered for release on licence/curfew.[210] These are used to risk assess the prisoner.[211] A PNC terminal is installed in some prisons and those without access are entitled to ask the nearest prison with access to provide them with the details they need.[212] A Public Accounts Committee in 2006 expressed surprised that only 43 of 113 prisons had direct PNC access, and the Home Office conceded that this made matters more 'difficult' than universal access would.[213] A Freedom of Information request by *Unlock* in 2009 revealed that the number of prisons with access had increased to 47[214] but it appears that universal access has not yet been provided.

4.5.3 Child protection and MAPPA

Local authorities ('LAs') have had access to criminal records for the purpose of vetting possible foster and adoptive parents since the 1930s.[215] However, although still used for that purpose, the predominant modern use of PHOENIX by LAs is in the performance of their child safeguarding functions. Each LA has a statutory duty to safeguard and protect the welfare of children[216] and to make arrangements to promote co-operations between them and relevant partners[217] to ensure that children are protected from harm and neglect[218] and to protect their economic and social well-being.[219]

---

[209] S. Kyle, 'Risk assessment in pre-sentence reports' (2005) 169 Justice of the Peace 374
[210] Ministry of Justice, 'Operation of the Police National Computer' (1 March 1999), Order Number 0905, ch.2, 'Key Points'
[211] Above n.63, 76
[212] Above n.210, ch.1, para.1.1.2
[213] Committee of Public Accounts, *The electronic monitoring of adult offenders* (HC 997 2005 – 06, 64-I) Ev10
[214] Home Office, 'Freedom of Information request. PNC Access by Prisons' (FOI/61065 *What Do They Know?,* 2 September 2009) <https://www.whatdotheyknow.com/request/pnc_access_by_prisons#comment-29988> accessed 22 August 2018
[215] Above n.63, 85
[216] Per s.11(1) and s.11(2)(a) of the Children Act 2004
[217] Ibid, s.10(1)(a – b)
[218] Ibid, s.10(2)(b)
[219] Ibid, s.10(2)(e)

One such 'relevant partner' is the appropriate chief police officer.[220] This means close co-operation between the police and social services, who work together to safeguard children primarily through the child protection case conference ('the CPCC') process. Where concerns regarding a child's welfare are raised by social services, an initial CPCC will be convened in order to 'bring together, in an inter-agency setting, all relevant information and plan how best to safeguard and promote the welfare of the child'.[221] This will often lead to police involvement and official guidance makes clear that 'the police will hold important information about children who may be suffering significant harm as well as those who cause such harm. They should always share this information with other organisations and agencies where this is necessary to protect children'.[222]

This usually means providing details of criminal records. The police have acted in this capacity since at least 1976, providing criminality data to CPCCs under the authority of various Home Office circulars.[223] Each force is able to determine a policy as regards the disclosure of criminal records, provided that they meet the national guidelines for data sharing and data protection legislation, but as an example, Wakefield Council and West Yorkshire Police's agreed current policy is that:

> Police information regarding criminal history and convictions and intelligence is often directly relevant to assessing risk to children and within the home environment. This information will be shared at conferences unless there is a circumstance which may compromise operational or criminal investigations.[224]

Less arrangements for the sharing of criminality information between the police and other agencies have existed for decades: West Yorkshire Police and their probation counterparts had a data sharing arrangement during the 1980s which attracted national attention[225] and which went beyond the simple sharing of information for operational purposes but rather involved the disclosure of criminal information as a means to try and prevent crime among known offenders.

---

[220] Ibid, s.10(3)
[221] 'Working Together to Safeguard Children' (HM Government, July 2018) 47
[222] Ibid, 63
[223] Home Office, Non-accidental injury to children: the police and case conferences' (HO 179/1967)
[224] Wakefield & District Safeguarding Board, 'protocol for police attendance at Initial Child Protection Conferences' (October 2015), paras. 4.1 – 4.2
[225] Above n.63, 87

This 'informal' disclosure of criminal records information by the police non-police agencies and members of the public as a means of actively preventing potential criminality was approved, in tentative terms, in *R v Chief Constable of North Wales ex. parte Thorpe*[226] where local police received a report from another force warning them that two particularly dangerous and notorious paedophiles had moved to a caravan site in the area.[227] After extensive discussions between both police forces, the probation service, social services and the applicants themselves, the recipient force decided it appropriate to disclose, prior to the Easter school holidays (and the resultant influx of children),[228] to the owners of the caravan site that two particularly recidivistic paedophiles were living on the site.[229]

The Court of Appeal upheld the police decision to disclose. They held that the police have an 'overriding duty to protect the public, particularly children and vulnerable people'[230] so that although 'disclosure should be made only where there is a pressing need for that disclosure'[231] it may be justified if it is required to fulfil the police's overriding duty.[232]

This decision provided the impetus to create more formal arrangements for sharing and disclosing criminal information to the public through 'Multi-Agency Public Protection Arrangements' ('MAPPA'). MAPPA were created by the CJA 2003[233] and provide a statutory obligation on the police and other agencies, such as HM Prisons and Probation, local housing authorities, the Department for Work and Pensions and social services, to 'assess and manage the risk provided by certain offenders'.[234] It does this by designating three categories of offender who require monitoring: specified sexual offenders, specified violent offenders and 'dangerous offenders'.[235] At March 2017, there were 76,749 MAPPA offenders[236] and where an offender falls within the ambit of

[226] [1998] 3 WLR 57
[227] Ibid, 62 [D]
[228] Ibid, 63 [D]
[229] Ibid, 62 – 63
[230] Ibid, 68 [B]
[231] Ibid, 68 [E]
[232] Ibid
[233] Per ss.325 – 327 of the Criminal Justice Act 2003
[234] Ministry of Justice, 'Multi-Agency Public Protection Arrangements, Annual Report 2016/17 (Office for National Statistics October 2017) 1
[235] Ibid, 1 – 2
[236] Ibid, 5

MAPPA, the police may elect to disclose to non-police individuals and agencies details of the offender's criminal record in order to prevent the offender committing new offences.[237]

The decision in *Thorpe* attracted little academic or media attention and it is outwith the scope of this article to offer a detailed evaluation of the merits, or otherwise, of that decision or the MAPPA processes which followed it.

However, some comments might be made. It is submitted that disclosures made under MAPPA will almost inevitably have far reaching consequences for those subjected to them. In *Thorpe*, the couple in question eventually fled the caravan site and 'went to ground, their whereabouts not known to the authorities' by the time the appeal was heard.[238] It cannot be conductive to the authorities to have known sex offenders 'go to ground' where they cannot be monitored effectively. Equally concerning is the possibility for vigilante action which now routinely follows the disclosure of such information. In the midst of the current 'paedophile panic', the revelation to the public that a convicted paedophile is nearby might trigger violent and dangerous repercussions.[239]

Even where MAPPA interventions are able to track offenders, there have been instances of serious reoffending. One instance in 2009 saw an offender under a MAPPA commit the murder of a seventeen year old girl.[240] This illustrates that, ultimately, the MAPPA process suffers similar problems to the (strikingly similar) 'ticket of leave' system over a century ago, namely that 'however stringent the…oversight of the MAPPA process, there will still be periods of each day and night when the individual has a degree of autonomy of movement – and a determined criminal will find a way to reoffend'.[241]

[237] A pamphlet has even been produced to be distributed to those who receive this sensitive information which warns that they should use the information provided to ensure that they are safe but not tell anyone else about the information they are given: see MAPPA, 'Disclosure of Information Leaflet' (2008)
[238] Above n.226, 63 [H]
[239] C. Baldwin, 'The Vetting Epidemic in England and Wales' (2017) (2012) 81(6) Journal of Criminal Law, 478, 488
[240] T. Thomas, 'Much ado about MAPPA' (2011) 175 Justice of the Peace 755
[241] M. Gosling, 'We know where you are' (2007) 171 Justice of the Peace 850

What is notable is that those subject to MAPPA are so subjected because they commit serious offences and the offending is recent to the MAPPA intervention. There is no suggestion that MAPPA would be utilised to deal with those convicted of minor offences, cautioned for similar offences or where those convicted have not come to police notice for any relevant period of time. In short, the removal of old and minor criminality data would have, it is submitted, a minimal impact on the MAPPA process. This ought to be borne in mind when contemplating the analysis offered in chapters seven and eight regarding the fourth research question.

4.5.4 Other PHOENIX data utilisation

PHOENIX use outwith the above listed purposes is very extensive, and it would be impractical to attempt to provide an exhaustive list here. Instead the author intends to provide an illustration of some of the more prevalent alternative uses.

Criminal convictions have a long history of use for national security purposes which can be traced back to the early years of the Cold War. This has meant an enhanced background screening of people working in Government or in other particularly sensitive posts.[242] After many years of vetting by a disparate collection of independent agencies, the predominant organisation responsible for security vetting is now the UK National Security Vetting which was launched on 1 January 2017. Vetting for National Security involves, among other elements, a check of the PHOENIX collection.[243] Other organisations who have direct access to the PNC for national security vetting include the National Air Traffic Systems Ltd, despite their having no legal authority to do so between 2006 – 2016.[244]

The Royal Mail is another longstanding user of PHOENIX data, having first had access to criminal conviction data in 1975 to assist them in bringing private prosecutions against those who commit offences against Royal Mail Group.[245] PNC terminals were installed in the mid-1990's into the investigative department of Royal Mail Group and

[242] Above n.63, 80 – 81
[243] United Kingdom Security Vetting, 'National Security Vetting: Advice if you are being vetted by us' (February 2018) 2
[244] Her Majesty's Inspectorate of Constabulary, 'Use of the Police National Computer by non-police organisations: An inspection of Air Traffic Systems Ltd (May 2016) 6 – 8
[245] Her Majesty's Inspectorate of Constabulary, 'Use of the Police National Computer by non-police organisations: A pilot inspection of Royal Mail Security Group' (May 2016) 4

the PIAP later re-approved 'read and update access'.[246] PHOENIX is broadly used in the same way that the CPS use it during the preparation and bringing of prosecutions,[247] though an attempt was made in June 2014 to persuade the PIAP to allow PHOENIX to be used as a simple employee screening tool. The PIAP refused to allow this and an appeal was unsuccessful.[248]

Similar provisions are provided to the Post Office, who have a single PNC terminal which provides direct access to PHOENIX[249] which is used so infrequently that the audit team who inspected them wondered whether they needed retraining to encourage greater use,[250] the Environment Agency[251] and the Financial Conduct Authority, who used their direct access to pursue prosecutions but also to check the criminal history of people applying for positions in the financial sector and people named in consumer credit applications despite having no valid authority to use the PNC for almost two years between 2014 – 2016.[252] Other organisations as disparate as Thurrock Council[253] and the Gangmasters Licencing Authority[254] also have access for crime investigation purposes.

Youth Offending Teams, responsible for dealing with juvenile offenders, are provided information from the PNC by police to assist them in their work.[255] The Children and Family Court Advisory and Support Service use PHOENIX to help them in their child safeguarding duties.[256] PHOENIX data is used to vet potential jurors.[257] Those who make a claim for compensation through the Criminal Injuries Compensation Scheme

[246] Ibid
[247] Ibid, 10
[248] Ibid, 13
[249] Her Majesty's Inspectorate of Constabulary, 'Use of the Police National Computer by non-police organisations: An inspection of Post Office Ltd' (May 2016) 4
[250] Ibid, 11
[251] Her Majesty's Inspectorate of Constabulary, 'Use of the Police National Computer by non-police organisations: A pilot inspection of Environment Agency' (May 2016) 6
[252] Her Majesty's Inspectorate of Constabulary, 'Use of the Police National Computer by non-police organisations: An inspection of the Financial Conduct Authority' (May 2016) 8
[253] Her Majesty's Inspectorate of Constabulary, 'Use of the Police National Computer by non-police organisations: An inspection of Thurrock Council (May 2016) 4
[254] Her Majesty's Inspectorate of Constabulary, 'Use of the Police National Computer by non-police organisations: Gangmasters Licencing Authority (May 2016) 6
[255] I. Walters, 'The police, young offenders and intelligence-led policing' (2006) 79(4) Police Journal 305
[256] Her Majesty's Inspectorate of Constabulary, 'Use of the Police National Computer by non-police organisations: An inspection of the Children and Family Court Advisory and Support Service' (May 2016) 8
[257] Code for Crown Prosecutors, 'Jury Vetting: Overview of Jury Checks' (7th edn, Crown Prosecution Service 2013)

will be subjected to criminal record checks and may face a reduction in, or a refusal of, any award if such a record exists.[258] The rules are applied *very* stringently and have given rise to criticisms in the media after victims of sexual offences were refused payments because they had criminal records.[259]

Each of these miscellaneous uses of PHOENIX arise because of the availability of the data and because the organisations involved are permitted to use it. It is submitted that none would be prejudiced were old and minor criminality data removed from PHOENIX.

4.6 Conclusions

The justifications for a central collection of criminal records relate directly to how they are subsequently used. They are important because any recommendation on how records are to be collected, what should be collected and who should have access must take into account all of the predominant uses for criminal records.

The precise nature of usage has proven to be malleable and oft-changing. Historically, the police, custodians of the PHOENIX data repository, have determined the justification(s) for retaining their criminal records; ordinarily posited as one or more 'operational policing purpose'. However, the last two decades have seen a marked increase in the scope of criminal record use at the behest of Parliament, who have expanded the use of PHOENIX to include criminal trials, punishment, and pre-emptive public protection, among others. One natural question is to wonder why these supposedly important uses for criminal records took until the 21st century to come to fruition and it is possible, indeed it is submitted that it is likely, that in truth, the government set itself to using a database which had been installed at public expense to the tune of tens of millions of pounds. In short, the suspicion remains that records are being used simply because they are available to be used.

Moreover, it is submitted that none of the justifications cited decisively determines that a complete record of all criminal disposals must be kept. Some, such as national security vetting, may appear more persuasive than others, but there is no substantive evidence to

[258] Ministry of Justice, 'The Criminal Injuries Compensation Scheme 2012' (The Stationery Office 2012) Annex D: Previous Convictions
[259] H. Agerholm, 'Rape victims with records of minor offences regularly denied compensation' *The Independent* (London, 5 April 2017)

prove that a person with a reprimand as a child on their record is a greater threat to national security than someone who does not. It is merely ‘presumed’ to be so. Likewise, the police justifications are very vague, do not appear to be evidence-based and rather demonstrate a continued deference to the police on operational matters which prior instances of police misconduct shows to be misplaced. Others, such as the use of PHOENIX information for bad character, as a statutory aggravating sentencing factor and as a disclosable fact relevant to civilians who live near sex offenders are very controversial and it is perfectly foreseeable that a different government with different views on criminal justice might entirely abandon some, or all, of them. In any event, each of these would not necessarily be impeded even in their present form if old, minor or juvenile data was to be removed from the PNC, or, at least, the argument that they would be so impeded is not immediately apparent.

The author submits, therefore, that although these justifications must be borne in mind when considering the nature of the record collection, there is little in them, individually or cumulatively, which determines that all records must be retained indefinitely, as matter of law, policy or even ‘common sense’. An argument can be advanced against such a proposition in every instance. This is the essential context for the analysis which follows in chapters 7 – 9 of this thesis, without which the fourth research question cannot be properly addressed.

5

The national collection of criminal records and compliance with the Data Protection Act 1984

5.1 Introduction

Until 1967, the Metropolitan Police had a statutory obligation to collect a register of offenders. The reality, as has been seen, is that the Metropolitan Police were effectively provided with *carte blanche* to obtain, and retain, whatever criminality information they chose, subject to any potentially narrow limitations prescribed by the law of tort. Indeed, a Home Office minister neatly summarised the Government's position in 1960 as being that: 'the Home Secretary's responsibility is confined to a power to prescribe the form in which criminal records should be kept in the central register and the particulars which should be kept'.[1] To otherwise interfere in the mechanisms of police investigatory work was considered an assault on police independence – unconstitutional, no less – and 'a very important principle and a safeguard against the creation of a police state [which] should, of course, be retained in full force'.[2]

Though broadly still maintained as principle, the advent of computerisation, and the concurrent potential for far greater record collation, storage and use, have seen numerous attempts to control, if not erode, the ability of the police to compile their criminality database. These have broadly focused on two separate, but intrinsically correlated, modern legal concerns: the right of individuals to respect for their privacy, and the need for those in charge of sensitive data to protect it, and in turn, protect those to whom the data relates.

In attempting to directly address the second research question, this chapter aims to offer a critical evaluation of the data protection questions which arose around the enormous repository of police criminality data held on PHOENIX as the first data protection legislation was enacted. The research will identify how criminal records were collated, stored and maintained during the relevant period before making before considering whether those responsible acting concordant with the applicable legal protections afforded

[1] HC Deb 27 June 1960, vol.627, col.1112
[2] HL Deb 8 December 1958, vol.213, col.23

by data protection legislation. It will conclude by examining the potential ramifications of the failure to bring those responsible for data breaches to account.

5.2 Home Office resistance to data protection legislation

By the turn of the 1970's, the potential improvements in cost, storage and speed of computerising manually held record collections were obvious even to MP's. However, those benefits were seen as being, at least by some Parliamentarians, offset by the civil liberty implications of larger and more intrusive central databases and the increased potential for damaging 'leaks' of data, particularly those involving 'personal information'.[3]

There followed a number of abortive attempts to try and curb the seemingly unfettered expansion of computerised databases. The first came in 1967, when Alexander Lyon MP introduced a bill which would have made an unreasonable and serious interference into personal privacy a cause of civil action, recoverable in damages.[4] It was denied a second reading amidst claims that it might restrict press freedom.[5] In 1970, Brian Walden MP introduced a bill which would have defined 'privacy' and put the protection of it on a legislative footing.[6] It attracted considerable support but encountered strong opposition from the Home Office, who persuaded Walden to withdraw the bill so that a Royal Commission could consider the issue.

The resultant Younger Committee (1972) were instructed to investigate whether legislative safeguards were required to protect privacy in light of the growth of computerised data,[7] but it was forbidden from considering public sector databases, including the imminent PNC, despite repeated lobbying to the Government to extend its remit.[8] The Government announced another consultative exercise in response and said a White Paper would be issued, but, according to Campbell and Connor, 'a general election conveniently intervened before further action was needed'.[9]

[3] HL Deb 3 December 1969, vol.306, col.103 – 105
[4] HC Deb 8 February 1967 vol.740, col.1565
[5] Ibid, col.1569
[6] HC Deb 23 January 1970, vol.794, col.959
[7] K. Younger, *Report on the committee on privacy* (Cmd 5012, 1972)
[8] HL Deb 6 June 1973, vol.343, cols. 105 – 06
[9] D. Campbell and S. Connor, *On the Record: Surveillance, Computers and Privacy* (Michael Joseph Ltd 1986) 25

Another MP, Leslie Huckfield, attempted twice to advance a 'Control of Personal Information Bill' which aimed to provide a regulatory framework for the supply and control of personal data in 'databanks', overseen by a tribunal which would provide 'licences' to those holding data on 100,000 or more subjects.[10] The first attempt in 1971 gained no traction at all, and while the second in 1972 fared better, it fell at the second reading stage.[11]

In 1974, the Government promised to publish a White Paper on potential data safeguards,[12] but it was repeatedly delayed until eventually it was published in 'less than the usual vague terms' and not much more became of it.[13] Another committee, this time headed by Norman Lindop, was convened in 1976 to look again at the issues of data protection and privacy, albeit encompassing both private and public sectors.[14] The final report, which recommended that an independent, statutory Data Protection Authority be set up and authorised to enforce a range of legally enforceable Codes of Practice with full legal powers of search and seizure, alarmed the Home Office so much that it was withheld for six months before it was finally released into the Commons library.[15]

The Government and the Home Office responded to Lindop's detailed recommendations by completely ignoring them and instead issued yet another consultation; a process which saw them 'consult all the people who had previously been consulted and who were concerned, all over again'.[16]

The reality which was now apparent was that successive Governments were actively hostile towards 'data protection'. Their only genuine concern regarding data was that it was 'secure', so that only the data owner (or those authorised by them) were able to access it.[17] Similarly, the Home Office wanted data protection legislation 'like they wanted a hole in the head'.[18] When asked whether legislation would be passed to allow citizens access to the records held against them on the PNC, the Home Office simply replied;

[10] HC Deb 21 April 1972, vol.835, col. 697 – 8
[11] Ibid, col.1010
[12] HL Deb 27 January 1975, vol.356, col.305 – 6
[13] Above n.9
[14] N. Lindop, *Report of the Committee on Data Protection*, (Cmd 7341, 1978)
[15] Above n.9, 26
[16] HL Deb 20 January 1983 vol.437, col.1538
[17] HC Deb 9 November 1972, vol.845, col.1190 – 91
[18] Above n.15

'no.'[19] Indeed, such was the obfuscation of the Home Office, a House of Commons Home Affairs Committee convened in 1979[20] to investigate the absolute lack of progress found that, since 1967, the Home Office's data responsibilities had been examined by no less than forty Royal Commissions and other committees for the net product of seventeen different reports resulting in zero legislative developments.[21]

Ultimately, events overtook the Home Office. On 28 January 1981, the *Convention for the Protection of Individuals with regard to Automatic Processing of Data* ('the 1981 Convention') was opened for signature by the Council of Europe.*[22]* The 1981 Convention established various safeguards regarding the 'quality'[23] and 'security'[24] of personal data, created a right of subjects to access data relating to themselves[25] as well as imposing a duty on signatories to instigate an 'authority' responsible for the general oversight of data and compliance with the Convention.[26] The UK signed on 14 May 1981 but could not ratify it until it passed the necessary domestic data protection legislation.[27]

There existed a special provision relating to collections of criminal records, namely that these could not be 'automatically processed' unless domestic law provided appropriate safeguards.[28] In this context, 'processed automatically' referred specifically to operations carried out 'by automated means': i.e. computerised collections.[29] This was therefore beneficial to the Metropolitan Police: although the 1981 Convention might apply to the PNC, it did not apply to the National CRO collection of criminal records, which remained in paper form at that time. And, in any event, even had the provision applied, it is likely that the police would have sought to derogate such an obligation as being 'necessary in a democratic society in the interests of public safety or the suppression of criminal offences'.[30] The net result was that the 'police were effectively exempt'.[31]

---

[19] HC Written Answers 25 May 1972, vol.837
[20] House of Commons Home Affairs Committee (1979 – 80, 1-I)
[21] Above n.9, 27
[22] Strasbourg Convention, European Treaty Series No.108
[23] Ibid, ch.II, Art 5
[24] Ibid, ch.II, Art.7
[25] Ibid, ch.II, Art.8(b)
[26] Ibid, ch.IV, Art.13(2)(3)
[27] Ibid, ch.II, art. 4 (1)(2)
[28] Ibid, ch.II, Art.6
[29] Ibid, ch.I, Art.2(c)
[30] Permissible under ch.II, Art.9(2)(a)
[31] B. Hayes, 'A Failure to Regulate: Data Protection and Ethnic Profiling in the Police Sector in Europe' (2005) Open Society 32, 33

It is not entirely clear why the Government signed the 1981 Convention; doing so effectively 'put a pistol to the Government's head'.[32] It is submitted that the likely reason was that the 1981 Convention forbade the transfer of personal data to or from a signatory country to a non-signatory country.[33] This created serious commercial concern that UK businesses might not be able to trade with companies in signature countries.[34] Reports began to surface in the media that UK companies were uncompetitive with international competitors because the UK did not have comparable data protection legislation with eleven other Western nations. Assurances were sought in Parliament[35] but when the Home Office tried to deny there was a problem, they were openly contradicted by business leaders.[36] The net result was an unlikely alliance of industry, trade unions, consumers, civil libertarians and commerce all calling for domestic legislation.[37]

Then, on 9 February 1982, *The Sun* reported that they had hired private detectives to obtain personal information relating to Michael Meacher MP,[38] who had a matter of weeks earlier made (yet another) abortive attempt to introduce data protection legislation via a Private Members Bill.[39] The private detective obtained a detailed cache of personal information. In response to Meacher's complaints at Prime Minister's Questions, and in a speech which allegedly 'stunned and dismayed' the Home Office, [40] Margaret Thatcher informed him that 'the Home Secretary will be introducing a White Paper this year. We agree that legislation is urgent. I hope that it will come forward in the next session of Parliament'.[41]

5.3 The Data Protection Act 1984

Perhaps the only organisation as openly hostile as the Home Office to the possible implementation of data protection legislation were the Metropolitan Police. The first 'interim guidance' on the PNC, produced by the Home Office in 1976[42] contained only one part of one sentence – a comment that police would aim to 'limit data held to the minimum

[32] Above n.16, col.1538 – 9
[33] Above n.9, 28
[34] J. Agar, *The Government Machine: A Revolutionary History of the Computer* (MIT Press 2003) 366
[35] HC Written Answers 16 June 1980, vol.986
[36] *The Times* (London, 21 July 1980)
[37] Above n.16, col.1539
[38] Above n.33
[39] Above n.9, 79
[40] Above n.9, 29
[41] HC Prime Minister's Question) 9 February 1982, vol.17, col.858
[42] Home Office, 'Privacy Precautions for Computer Systems Handling Personal Data' (1976)

necessary' – which related to any data protection concern other than ensuring that the data was 'securely stored'. This *laissez-faire* approach arose because, according to Campbell and Connor, the Home Office and the Metropolitan Police presumed that the PNC and any other police system would be exempt from any potential data protection legislative provisions.[43]

This belief that 'wide exemptions' would be given to the police, and especially the Metropolitan Police, was echoed by Lindop after they were called to give evidence before his Committee and effectively refused to provide detailed response to issues raised.[44] The Metropolitan Police sent three officers, including the Assistant Commissioner, who opened their evidence by informing the committee that they thought the panel unnecessary and untrustworthy, telling the chair that 'there are members of your committee whose loyalty we cannot take for granted'.[45] The police then refused permission to record their evidence.[46] When questioned about possible data protection legislation, the three police officers stated simply that if data protection legislation was to be brought, that they should be exempted from it.[47] It is perhaps not surprising, therefore, that Lindop felt moved to write in protest (in vain) to the Home Secretary about the attitude of the police[48] and note in the committee's final report that the Metropolitan Police had been 'particularly unhelpful to their enquiries'.[49]

All of this notwithstanding, the Home Office now had little choice but to produce domestic data protection legislation. Their aim was to 'do the bare minimum to satisfy the 1981 Convention'.[50] The result, after another White Paper[51], another General Election and two more bills,[52] was the Data Protection Act 1984 ('the DPA 1984'),[53] which received Royal Assent in July 1984.

[43] Above n.9, 307
[44] Above n.14, paragraph 8.03
[45] Above n.9, 37 – 8
[46] Above n.9, 37
[47] Above n.3
[48] Above n.9, 38
[49] Above n.44
[50] C.N.M Pounder, 'Data Protection and the Police' (1983) Journal of Law and Society 10 109, 115
[51] Home Office, *Data Protection: The Government's Proposals for Legislation* (Cmd 8539, 1982)
[52] The Data Protection Bill (1982 – 83) and The Data Protection Bill (June 1983). Both were heavily criticised throughout their journey through the legislative process. These criticisms are somewhat outwith the remit of this research: see above n.9, 30 – 38 for a comprehensive treatment of these.
[53] 1984, ch.35

The DPA 1984, like the 1981 Convention before it, referred specifically to 'personal data': data consisting of information which relates to a living individual who can be identified from that information'.[54] Criminal records, of the kind retained by the CROs, would unquestionably fall within this definition. The DPA 1984 instituted a Data Protection Registrar ('the Registrar'),[55] whose role included receiving the new, mandatory registration[56] of 'data users'[57] or those operating 'computer bureaux'[58] and compiling these into a publicly inspectable 'Register of Data Users'.[59] The registering body was required to provide to the Registrar, among other details, a description of the personal data held by them and the purpose they were holding it.[60]

Schedule 1 of the DPA 1984 provided eight general 'Data Protection Principles'. These provided that (in slightly abridged form):

1. Personal data shall be obtained, and processed, fairly and lawfully;
2. Personal data should be held only for one or more specified and lawful purpose;
3. Personal data shall not be used or disclosed in any matter incompatible with that purpose;
4. Personal data shall be adequate, relevant and not excessive in relation to that purpose;
5. Personal data shall be accurate and up-to-date;
6. Personal data shall not be held longer than necessary for the stated purpose(s);
7. Individuals are entitled to know if data is being held, to access copies of it ('subject access') and, where appropriate, to have it corrected or erased;
8. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure, destruction or accidental loss of personal data.

Failure by any registered body to comply with the principles entitled the Registrar to issue an 'enforcement notice' requiring that the failure be rectified.[61] The Registrar had a (limited) power to seek a warrant from a circuit judge to enter and inspect premises where

[54] Per Part I, s.1(3) of the Data Protection Act 1984
[55] Part I, s.3(1) of the Data Protection Act 1984.
[56] Per Part II, s.4(1) of the Data Protection Act 1984
[57] Defined in Part I, s.1(5) of the Data Protection Act 1984
[58] Defined in Part I, s.1(6) of the Data Protection Act 1984
[59] Above n.54
[60] Per Part II, s.4(3)(b) of the Data Protection Act 1984
[61] Per Part II, s.10(1) of the Data Protection Act 1984

suspected breaches were taking place[62] but s/he could only act in receipt of a complaint.[63] Failure to comply with an enforcement notice was an offence.[64]

It had been expected (not least by the police themselves) that the police would benefit from wide ranging exemptions to the DPA 1984.[65] The Lindop Committee, perhaps unsurprisingly given their experience with the Metropolitan Police, were of the contrary view, namely that 'any…exemptions from the DPA 1984 should be precisely limited to national security. Police records…having no bearing on national security, should not be exempted'.[66]

The DPA 1984 did contain provisions which protected the police from certain obligations. Personal data held for the purposes of the prevention or detection of crime[67] or the apprehension or prosecution of offenders[68] was exempt from 'subject access'.[69] This reflected the Parliamentary view that 'to provide a data subject with access to his file, where the file relates to police suspicions of his criminal activity, would be nonsense'.[70] Additionally, an exemption to (almost all) of the protections of the DPA 1984 was provided in the interests of 'national security'. Such exemption was granted if a certificate, signed by a Minister of the Crown, was obtained confirming that the exemption was approved.[71] This has led to one academic suggesting that 'national security' provided a catch-all exemption to the Act and that subjects had 'no rights of access' to information on the PNC.[72]

This author respectfully disagrees. In the course of this research the author has found no substantiating evidence to support those claims. Indeed, the contrary position appears the correct one. Certainly, Lindop made a clear distinction between 'national security' and 'police records' and it is difficult to envisage that a list of someone's criminal convictions might ordinarily involve a matter of national security. Indeed, the true position was

[62] Per Sch.4, s.1 of the Data Protection Act 1984
[63] Per Part V, s.36(2) of the Data Protection Act 1984
[64] Per Part II, s.10(9) of the Data Protection Act 1984
[65] Above n.50, 115
[66] Above n.14, paras.38.51 – 38.53
[67] Per Part IV, s.28(1)(a) of the Data Protection Act 1984
[68] Per Part IV, s.28(1)(b) of the Data Protection Act 1984
[69] Per Part IV, s.28(1) of the Data Protection Act 1984
[70] HC Deb 11 April 1983, vol.40, col.558
[71] Per Part IV, s.27(1)(2) of the Data Protection Act 1984
[72] A. Hoey, 'Techno-cops: Information Technology and Law Enforcement' (1998) 6(1) International Journal of Information Technology 69, fn.14

probably that the DPA 1984 was: 'more effective in the case of the police than envisaged by critics'.[73] The right to subject access of PNC records was subject to exemptions, certainly, but exemptions to the general principle that there existed a right to subject access.

It was certainly Parliament's view that the police, and their PNC, would be subject to the DPA 1984. The Home Secretary told the Commons that: '…data held by the police for the purposes of crime prevention will be registered and accessible by the Registrar'.[74] Indeed, the police did register, as data users for both the PNC and their local force computer systems.[75] The true position, then, is that the police were as bound by the DPA 1984 as any other data user, subject to the limited exemptions in ss.27 – 28. This was confirmed in 1985, when Home Office minister Giles Shaw confirmed that:

> Under the provisions of the Data Protection Act 1984, individuals will have access to data on the police national computer which relates to them, subject to the condition that grant of access will not prejudice the prevention or the detection of crime, or the apprehension and prosecution of offenders. The Act also provides for the rectification and erasure of inaccurate data.[76]

So far as criminal records were concerned, however, there were caveats. Like the 1981 Convention which preceded it, the DPA 1984 only applied to computerised databanks.[77] The DPA 1984, therefore, applied generally to the PNC and the 'local police computers', which by 1982 were being operated by 39 of the 51 police constabularies.[78] It did not, however, apply to the paper-copy criminal records held at any of the CROs, nor did it apply to the collection of microfiche records.

It is submitted that this explain the (otherwise difficult to justify) decision to convert the criminal records to microfiche, rather than direct to the PNC. The programme to convert hard-copy records to microfiche commenced in 1980: the same year that the Council of

[73] Above n.43. The context suggests that 'effective', so far as the authors were concerned, meant 'restrictive'.
[74] Above n.70, col.558
[75] Above n.43
[76] HC Written Answers 28 June 1985, vol.81, col.519
[77] Per Part I, s.1(1) of the Data Protection Act 1984.
[78] See: HC Orders of the Day 1 April 1982, vol.21, col.532. These will be discussed in more detail in chapter seven of this research.

Europe were drafting their 1981 Convention. The police would, therefore, presumably be aware that the 1981 Convention would apply only to computerised databanks and that any subsequent legislation implemented in compliance with the 1981 Convention would likely also do likewise.

This submission might appear rather paranoid, but in giving evidence to Lindop, the Metropolitan Police threatened that the computerisation of criminal records would have to be 'abandoned' if data protection legislation was applied to it.[79] It also occurred to Parliament (while the legislation was being debated) that there was a possibility that data users would be encouraged to, at least, retain paper files over computerising records to avoid the provisions of the DPA 1984.[80] Indeed, as soon as the DPA 1984 came into force, computing organisations were advising their members on how to avoid the strictures of the Act: one guide advised simply that 'the simplest thing to do is to return information to the old-fashioned filing cabinet',[81] while the National Computing Centre, whose staff included Eric Howe (soon to become the first Data Registrar), provided a pamphlet which advised data users to 'keep records in a card index: you will be completely exempt'.[82]

The police decision to start adding complete conviction records onto the PNC in 1985 only for those convicted of a new recordable offence on or after 1 January 1981[83] should be considered in this light. A conscious decision was taken to leave older, 'inactive' records in abeyance, where the eight Data Protection Principles, nor any other DPA 1984 provision, would not be applied to them. Only the computerised criminal records added to the PNC after 1 January 1985 fell under the auspices of the DPA 1984.[84]

The DPA 1984 was in effect until it was repealed on 18 July 1998 and its provisions applied until that date. Since its inception, the police have been bound by statutory restraints imposed by the DPA 1984 on the collection and storage of criminal records held (only) on the PNC. These imposed positive legal obligations which the police were obligated to adhere to in order to ensure compliance with the data protection principles.

---

[79] Above n.14, para.8.29
[80] For one example, see above n.16, col.1552 – 1553
[81] N. Savage and C. Edwards, 'A guide to the Data Protection Act 1984' (Financial Training Publications 1985), cited in D. Campbell and S. Connor, above n.9, 318
[82] J.M Court, 'Personal Data Protection – the 1984 Act and it's implications' (National Computing Centre 1984) section 8.
[83] T. Thomas, *Criminal Records: A database for the Criminal Justice System and Beyond* (Palgrave MacMillan, 2007) 28
[84] HC Written Answers 3 May 1984, vol.59, col.208 – 09

5.4 Police compliance with the fifth DPA 1984 principle

Despite police claims regarding the hyper efficiency of the CRO and the completeness of their records, rumours suggesting that the criminal record collection might not be entirely accurate have persisted for decade; James Rule in 1970 noted that 'the system does not work perfectly…and some convictions go unrecorded'.[85]

The true position was that the national criminal record collection was in a parlous state. In *R v Kinsella*,[86] the Court of Appeal was forced to re-sentence a burglar when it transpired that the original disposal was made after consideration of antecedents which omitted a prior custodial sentence. Such omissions were not unusual. In giving evidence to a Home Affairs Committee convened to examine the work of the CPS, the London Criminal Courts' Solicitors' Association claimed that the criminal records at the NIB were so inaccurate that bail and sentencing hearings were routinely made on the basis of incorrect antecedents.[87] It described the practice of defence lawyers having to fill the gaps from their own knowledge of their clients as a 'very worrying state of affairs'.[88] The Law Society went even further, telling the committee that criminal records were 'in a terrifying state of inaccuracy' and that the number of instances where criminal records were wrong were 'very, very high indeed'.[89]

Media reports then emerged claiming that ministers were considering taking control of the criminal records from the police and entrusting them to an executive agency instead. The Registrar even said that he was in favour of so doing.[90] Meanwhile, a Home Affairs Committee were sufficiently alarmed by the apparent scale of the inaccuracies that they broke off from their analysis of the CPS to conduct a review of the criminal record collection first.[91] This found serious problems: it took an average of 77 days for the police to notify the NIB of new information to be added to the record and over 30,000 records were still incomplete after two and a half years.[92]

---

[85] J. Rule, *Private Lives and Public Surveillance* (Allen Lane, London 1973) 67
[86] *The Times* (London, 11 September 1990)
[87] C. Baldwin, 'The Vetting Epidemic in England and Wales' (2017) 81(6) Journal of Criminal Law 478, 482
[88] F. Gibb, 'Sentences based on inaccurate criminal records, MP's told' *The Times* (London, 22 February 1990)
[89] Ibid
[90] Q. Cowdry and M. Souster, 'Separate agency 'would ensure accurate records' *The Times* (London, 8 May 1990)
[91] Home Affairs Committee, *Criminal Records* (Cmd 285, 1989 – 90 3-I)
[92] Ibid, para.8

The problem was that the police maintained responsibility for adding material to the PNC long after their responsibility for the prosecution of offenders had ended; in some cases, the police were sending officers to court to take manual records of convictions to later add to the PNC.[93] The committee recommended that the Home Office issue urgent guidance to court clerks to speed up the flow of information[94] but that, when full computerisation was achieved, that court clerks be the inputters of the conviction data.[95]

The Home Office responding by announcing that an 'efficiency scrutiny' would be carried out to investigate further.[96] This report[97] found that the criminal record data was 'in a very unsatisfactory'[98] and 'a very fragile'[99] state and claimed that only full computerisation would solve the problem.[100] New deadline targets for updating records were issued; arrest data should be sent to the NIB within five days and court results sent within ten.[101] They also believed that an independent organisation should be created to oversee the record collection.[102] The Home Office finally published the six months after it was received, conceding that there was 'a need to improve the maintenance and use of the national collection of criminal records'.[103]

Some of the inaccuracies went beyond simple errors and a lack of timeliness. One record noted that the individual's 'left eye glides to the centre of his face, where it is stopped by his nose' when spoken to by police.[104] Such 'records' led NIB staff to report that they 'had a good laugh over the clangers…some officers aren't too particular when they're taking down particulars'.[105] Other criminal justice agencies weren't quite so amused; the chairwoman of the Magistrate's Association told the media in 1994 that criminal records presented in court 'were regularly defective' and a source of 'major frustration'.[106]

---

[93] Ibid, para.9
[94] Ibid, para.10
[95] Ibid, para.11
[96] HC Written Answers 28 November 1990, vol.181, col.420
[97] Home Office, 'The National Collection of Criminal Records: report of an efficiency scrutiny' (HC Library DEP 7158, 1991)
[98] Ibid, para.19
[99] Ibid, para.106
[100] Ibid, para.23
[101] Ibid, Annex M
[102] Ibid at para.48
[103] HC Written Answers 22 October 1991, vol.196, col.531
[104] 'Baffling case of gliding eyeball' *The Daily Mirror* (London, 22 April 1993)
[105] Ibid
[106] C. Dyer, 'Criminal record errors causing lighter sentences' *The Guardian* (London, 3 March 1994)

Despite the long-awaited computerisation of the records via PHOENIX 1995, the problems persisted. An internal review by the Police Information Technology Organisation ('PITO') in 1996[107] generated sufficient concern that they asked a Home Office Police Research Group to investigate the situation and make a report. This, published in 1998 after a two-year investigation,[108] was 'quite alarming in its findings'.[109] It found that computerisation, rather than providing the 'silver bullet' to improving the data quality as had been hoped, was making matters worse, because without the centralisation provided by the NIB, individual police officers were either unwilling or unable to input data accurately, completely or quickly.[110] Moreover, individual forces had adopted inconsistent policies for inputting data in accordance with their new PHOENIX roles and this meant a lack of quality control regarding accuracy, timeliness or completeness.[111] Remarkably, police officers confessed to 'making up' information where they did not know, or could not remember, the correct data.[112]

The inspection found that the time taken to record an arrest on the PNC could be 'many weeks'.[113] Other key agencies, such as the Magistrates and Crown Courts, were equally culpable, with one force reporting that the delay in getting conviction disposal data from one Crown court was up to twelve months.[114] The result was continuing reliance on incomplete antecedents; one suspect was granted court bail as a first-time offender only for it to later transpire that he had six previous convictions 'sitting in the police backlog'.[115] Seven recommendations for improvements were made, including the introduction of national standards for timeliness, the creation of a 'national format' for data input to ensure consistency and greater accountability for errors to individual and senior officers. It also recommended that officers be provided with more training on the 'benefits' of the

[107] Police Information Technology Organisation, 'A review of Phoenix input standards and data quality' (1996)
[108] J. Russell, 'Home Office Police Research Group Special Interest Paper 11 – Phoenix data quality' (HC Library Dep 98/183, 9 April 1998)
[109] K. Povey, 'On the record; thematic inspection report on police crime recording, the police national computer and Phoenix Intelligence System data quality' (HMIC July 2000) 75
[110] J. Russell, 'Special Interest Paper No.11 – Phoenix Data Quality' (Home Office Police Research Group March 1998), quoted in Select Committee on Home Affairs, *Criminal Records* (HC 227, 2000–1 2-I) [23]
[111] Select Committee on Home Affairs, *Criminal Records* (HC 227, 2000–1 2-I) 26
[112] Ibid, 8
[113] Cited ibid, Appendix 8 [2]
[114] Above n.109, 31
[115] Ibid, 33

PHOENIX collection to alleviate the prevailing attitude among officers that it was little more than an administrative burden, rather than an investigative tool.[116]

It was not just those in the criminal justice system who suffered as a result of inaccurately held records. Adverse consequences began to filter down to innocent individuals caught up by the parlous state of the records on the nominal index. In October 1986, one woman was refused a position in a special programme for delinquent teenagers after police mistook her for another person who shared the same maiden name and disclosed that person's criminal record.[117] In 1990, an innocent man named Neil Foster found himself wrongly arrested and charge for driving whilst disqualified when, in fact, the disqualified man in question was an entirely different Neil Foster. The truth only emerged at a magistrates trial, at which the innocent man was acquitted, by which time he had lost his job, his car and spent thousands in legal fees.[118] In 1995 another man found that the PNC contained two recorded offences against his name, which he denied having ever been convicted of, when he was refused employment at the local council. In a remarkable admission, the chief superintendent of the police force which held the record said that 'bosses should not assume that records are accurate'.[119]

What is clear is that, by the early 1990s at the latest, there was widespread knowledge that there existed 'a serious problem concerning the accuracy of these records'[120] with magistrates describing that 'the problem of obtaining up-to-date convictions is nationwide'.[121] What is not clear is why the Registrar did not intervene and issue enforcement notices against chief police officers and/or the NIB for what appear to be *prima facie* breaches of the fifth DPA 1984 principle. The Registrar certainly knew that the problems existed. In his 1991 annual report, he referred explicitly to the 'efficiency scrutiny' of the criminal records[122] and made explicit comment of its report in his 1992 report, where he claimed to be 'pleased to note the recognition of data protection requirements' and that, overall, he 'welcomed the report'.[123]

---

[116] Ibid, 205 – 206
[117] Police find a Catch-22 for data victim *The Guardian* (London, 8 October 1986)
[118] M. Souster, 'Innocent man in case of mistaken identity' *The Times* (London, 8 May 1990)
[119] 'Branded a thief and barred from a job' *The Daily Record* (Glasgow, June 20 1995)
[120] M. Colvin, 'The Criminal Record and Information System in England and Wales' (1992) 6 International Yearbook of Law Computers and Technology 141
[121] Editorial (February 1994) 50(1) The Magistrate 20
[122] The Data Protection Registrar, 'The eighth report of the Data Protection Registrar' (HMSO June 1992) 6
[123] Ibid, 7

Quite why he was so effusive about a report which laid, in the clearest and most damning manner, the paucity of the police's attempt to fulfil their data protection obligations is not immediately clear. Certainly, he made no mention of the problems in his 1992 supplemental comments relating to the retention, use and disclosure of criminal data and seems to have neglected to note that the very thing which triggered the 'efficiency scrutiny' was that the collection of records was in an abominable state. Despite problems persisting throughout the remainder of the decade, the Registrar does not appear to have to taken any enforcement action against any chief police officer in respect of breaches of the fifth DPA 1984 principle.[124]

There do not appear to be many plausible explanations for the apparent inactivity on the part of the Registrar. One possible justification is that, despite the significant problems faced by those reliant on accurate criminal record data, it does not appear that any formal complaint was raised by any individual or organisation directly to the Registrar. This seems extremely unlikely: one report in 1990 seems to indicate that such complaints were, in fact, being made,[125] the Registrar himself confirmed in his sixth annual report that one complaint to him had involved the branding of an innocent individual as an attempted murderer in a nominal PNC record.[126]

These notwithstanding, if this is the explanation for his inactivity, then it is an unsatisfactory one. By 1994, ordinary members of the public who read newspapers knew that the criminal record collection contained countless inaccuracies. The Registrar certainly should have known, and in fact did know, the very same. That alone should have been sufficient to warrant his intervention. If he was waiting to receive a 'formal' complaint, then his inaction might at best be described as unduly timid.

A second possible explanation may be that, at this time, much of the collection remained in microfiche form; as has been seen, only those who came to police notice after 1985

[124] The Information Commissioner, 'FOI Request. Data relating to enforcement notices issued to police forces in respect of the nominal index of the PNC' (Case Ref: IRQ0772426 *What Do They Know?,* 1 August 2018) <https://www.whatdotheyknow.com/request/data_relating_to_enforcement_not#incoming-1221131> accessed 1 August 2018

[125] P. Large, 'Data error complaints double' *The Guardian* (London, 2 March 1990)

[126] Reported by M. Hughes, 'Now data watchdog fears for loses in the numbers game' *The Guardian* (London, 22 July 1990)

had their full records uploaded to the PNC, so several million records remained undigitized and, therefore, outwith the remit of the Registrar. That may be so, but by April 1996 some 2.1 million 'complete' criminal record *were* uploaded onto PNC2.[127] These should have included the antecedents of *Kinsella*, whose 'missing' disposal occurred in November 1989. These records *did* fall under the remit of the Registrar under the DPA 1984. When PHOENIX went live in 1995, the entire digital collection of records fell under the auspices of the DPA 1984. Once this occurred, the jurisdiction of the Registrar to act was confirmed entirely.

Whatever the reason for inaction, it is submitted that, by no later than the end of 1992, at least some chief officers were in *prima facie* breach of the fifth data protection principle. Moreover, it is equally clear that the Registrar failed to issue enforcement notices when s/he ought to have done so. It is further submitted that, by failing to intervene at an early stage, the Registrar (at least partially) facilitated a lack of police action to correct the deficiencies which would ultimately have significant ramifications in the decade to follow.

5.5 Police compliance with the eighth DPA 1984 principle

As has been shown, in the formative period of data protection, the predominant concern of the Home Office and the police was that data was 'secure' so that only the police, or those otherwise authorised, could access the criminal records. This concern largely stemmed from the widespread knowledge that the criminal records were not secure from unauthorised access at all, though the source of the data breaches lay not with thieves or computer 'hackers', but with the police themselves.

James Rule saw for himself the problems on unauthorised access to the criminal records in the 1970's. He described how 'virtually anyone familiar with the telephone number of the regional CRO and the routines for making such requests can eventually obtain the information he seeks; if not on the first try, then sooner or later'.[128] This meant that the system was particularly vulnerable to retired police officers who took up work as private detectives and were employed by businesses who, for whatever reason, wanted access to the records.[129] Retired officers, with their intimate knowledge of the system and close personal ties to others still employed at the CROs, were ideally suited to the task.

[127] Police National Computer, House of Commons (Written Answers) 3 April 1996, vol.275, col.285
[128] Above n.85, 82
[129] Ibid

The issue was reported to the Younger Committee, who were told that '99% of private detectives and inquiry agents would have access somewhere along the line to criminal records'.[130] When this was put to the Home Office, they told Parliament that the allegation 'was quite without foundation…the sources of information were not police sources'.[131] That unconvincing rebuttal seemed to fly in the face of what was becoming a well-publicised problem with data security; Lord Gardiner told the House of Lords in 1973 that the Home Office position was simply '…wrong. One knows it as an ordinary person, one knows it from company directors who tell one'.[132]

The issue clearly had not been much resolved by the following decade, as *The Sun* exposé of Michael Meacher's personal data in 1982 amply demonstrated. Another newspaper investigation resulted in the disclosure of information to journalists who 'fooled' CRO staff by loosely impersonating serving police officers.[133] After the implementation of the DPA 1984, the problems persisted. In 1988, a former detective constable was tried under the Official Secrets Act 1911 in respect of allegations that he passed criminal records to a private 'investigation agency'. He was ultimately acquitted[134] but an interesting insight was provided by a former chief superintendent, who testified on behalf of the defendant that he would condone leaking PNC information 'if it was consistent with his overriding duty to the public and society'.[135] In 1989, three more police officers were charged with offences under s.2 of the Official Secrets Act when a BBC documentary uncovered evidence that they were passing PNC data, including criminal conviction details, to five private detectives. All eight were convicted and handed suspended prison sentences of varying lengths.[136]

The case was sufficiently grave that ACPO promised to review access arrangements to the PNC to prevent misuse and alleviate concerns from the Registrar that data may not be secure.[137] This culminated in software upgrades in 1990 which logged officer ID's when

[130] Above n.7, para.436
[131] Ibid
[132] Per Lord Gardiner at HL Deb 6 June 1973, vol.343, col.121
[133] D. Leigh, 'Police give computer secrets out' *The Observer* (London, 4 October 1981)
[134] 'Police records 'were leaked'' *The Guardian* (London, 24 February 1998) and 'Leak verdict' *The Times* (London, 27 February 1988)
[135] 'Police leaks justified' *The Times* (London, 26 February 1998)
[136] Home News, 'Policemen guilty of conspiracy over computer information' *The Independent* (London, 3 February 1989)
[137] P. Evans and T. Dawe, 'Review of police security' *The Times* (London, 4 February 1989)

they accessed the PNC records, along with random checks by senior officers. The police claimed this made unauthorised use of the system far more difficult[138] and led the Home Office to claim that access to the records was provided only in 'tightly drawn circumstances.[139]

The Home Office's confidence proved ill-founded. In 1994, Scotland Yard was forced to launch an inquiry into what amounted to a 'thriving black market' of criminal records being sold by police officers to private detectives.[140] In 1997, a Metropolitan Police officer was jailed for two years for selling criminal records information relating to two hundred individuals to private investigators.[141] One week later, a *Sunday* Times investigation found serving police officers at Scotland Yard using their PNC access to set up investigating agencies to make extra money, while one detective constable offered to sell criminal records information from PHOENIX to an undercover journalist for fifty pounds, triggering yet another 'anti-corruption' inquiry involving senior officers.[142] In West Mercia, one serving and two former police officers were jailed in 1999 after the serving officer conducted unlawful 'background checks' on 19 people and passed the details to the others, who had set up an 'investigation agency'.[143]

It is likely that the police will say that they took 'appropriate' measures to protect data subjects from this series of data breaches so that they discharged their obligations under the DPA 1984. However, it is submitted that the sheer volume of instances where security was breached, coupled with the widespread knowledge that such breaches were commonplace stretching back to the 1960's, suggest otherwise. It is evident that *whatever* measures were taken by the police to prevent these breaches were ineffective; it seemed that after each breach, more serious than the next was uncovered, the subsequent inquiry concluded that new and more stringent countermeasures were to implemented, only for further breaches to be uncovered and this 'cycle' repeat almost *ad infinitum*.

[138] M. Souster, 'Officer says misuse is falling' *The Times* (London, 8 May 1990)
[139] HC Deb 2 February 1989, vol.146, col.412
[140] C. Stern, 'Crime files are stolen from national computer' *The Mail on Sunday* (London, 14 August 1994)
[141] 'Policeman jailed' *The Times* (London, 5 July 1997)
[142] D. Leppard, J. Burke and T. Kelsey, 'Corrupt police sell secrets in Yard scandal', *The Sunday Times* (London, 24 August 1997)
[143] 'Police pair jailed on files leak' *Birmingham Evening Mail* (Birmingham, 23 February 1999)

It is, therefore, not clear why the police were not issued with enforcement notices by the Registrar in respect of what appears to be a litany of *prima facie* breaches of the eighth data principle. One week after the conclusion of the 1989 trial which saw eight men convicted for selling PNC data, the Registrar gave a public speech condemning local authorities for asking unlawful questions on poll tax forms. He said nothing as regards the issues of unlawfully accessing, using or selling criminal records.[144] The subject is also conspicuously absent from all of his first ten annual reports. This, it is submitted, seems a remarkable omission. The author has deliberately selected media reports of data breaches in this section to highlight the *extremely* public nature of the debate regarding unlawful access and use of criminal records. It is inconceivable that the Registrar was not aware of the problem. To have a comprehensive knowledge of it all that was required the s/he read a newspaper.

Once again, it is submitted that, by his (presumably deliberate) inaction, this time deferring to the various provisions of the criminal law to 'deal' with the matter instead, the Registrar not only failed to deal with a matter of considerable public importance but also encouraged police officers to seek, and facilitate, unlawful use of criminal records contrary to the eighh data principle and allowed data controllers to take ineffective preventative measures, safe in the knowledge that legal action would lie only with the individual officer(s) responsible, not them, which in turn discouraged the development of more effective countermeasures.

5.6 Conclusions

The advent and growth of computerisation in the 1970's gave rise to new concerns regarding privacy and civil liberties. These were particularly pertinent to the Police National Computer, which had the potential to provide a systematic data repository on huge swathes of the population. Despite procrastination and obfuscation from the Home Office, and outright hostility from the police, the Data Protection Act 1984 was enacted to assuage fears and provide controls on what data could be collated, how and where it could be stored and what responsibilities the police had regarding the accuracy and security of that data.

What is evident is that the police, in the practices adopted by them in the collection, storage and retention of criminal records, appeared to be in *prima facie* breach of the DPA

[144] S. Crossland, 'A nation without secrets' *The Sunday Times* (London, 16 July 1989)

1984 in two regards. The accuracy of their records and the secure storage of them were both sufficiently problematic that investigations into matters which might reasonably be considered DPA 1984 breaches were carried out with an almost monotonous regularity; by the early 1990s both had become 'mainstream' news stories. These breaches were not 'trivial' in nature. They involved the unauthorised sale of sensitive personal data to unregulated individuals and meant that decisions in court regarding bail and sentencing were being made on the basis of factually inaccurate information. The former is an indefensible violation of an individual's civil liberties and right to personal privacy. The latter brings the entire criminal justice system into possible disrepute.

Despite the overwhelming evidence in support of taking action against the police, the Registrar, instituted to ensure compliance with the DPA 1984 and to protect the data subjects who fell within its ambit, elected to take no formal action. It is not clear why this approach was taken, although it is submitted that this might be explained by a (perhaps understandable) desire on the part of the Registrar not to 'ruffle the feathers' of an organisation who had forcefully repudiated the invocation of data protection principles to their work from the outset of their conception.

Whatever the explanation for it, it is submitted that the second research question can be answered in the affirmative. It is also further submitted that this timorous approach had two important consequences. The first is that it meant that thousands of data users were the subject of unpunished data breaches. Not unnaturally, those affected may feel that they have been denied the justice afforded to them by the implementation of the DPA 1984.

It is submitted, however, that the second consequence would be more damaging still. By not taking firm action against the police while data protection legislation was in its infancy, and while the police were still grappling with the new oversight supposedly offered by the Registrar, it is submitted that the Registrar facilitated the continuing police breaches of the DPA 1984. His (and latterly her) inactions emboldened the police to downplay the significance of data protection. By not acting, the Registrar provided no motivation to the police to improve the security of their records or to securely store them. It also discouraged them to 'weed' inactive minor records, as will be examined at length at chapter eight of this research. Such actions were time, labour and cost intensive and involved, so far as police were concerned, the diversion of valuable resources away from the 'core' functions

of the police into what some police believed to be ‘an administrative chore’.[145] It is easy, therefore, to imagine that the police would not undertake these tasks without an external imposition to do so placed upon them.

It is submitted that, in short, the Registrar’s failure to take action emboldened the police to believe that the protections afforded by the DPA 1984 applied to them in nominal terms only, if at all. The author further submits that this error on the part of the Registrar would become a very damaging one if, or indeed when, the Registrar finally elected to take the police to task and was unable to do so or if, or when, the failings of the police to properly control their data finally manifested into a failure to exercise their ‘core’ functions.

[145] Above n.92, para.7

6

Police compliance with the Data Protection Act 1998 in respect of the PNC PHOENIX application

6.1 Introduction

Outwith the provision for subject access, the introduction of data protection in 1984 did not bring any noticeable difference so far as criminal records were concerned. The police still had a seemingly unfettered discretion to collect an enormous amount of data regarding citizens and criminality, and to store and utilise it at their discretion. As outlined at length in the previous chapter, it is submitted that this was because the newly instituted Data Registrar showed an almost complete reticence to take the police to task, despite having numerous opportunities to do so as grievous examples of data breaches became apparent.

This chapter will attempt to address the third research question by taking a near-identical approach to the previous chapter of this research, but in respect of the data protection legislation which succeeded the DPA 1984. This will involve firstly an examination of the development and implementation of a new set of data protection principles, before, in common with the previous chapter, attempting to identify and critically evaluate further instances of the police's failure to adhere to the data protection principles and a critical analysis of the reaction of those charged with overseeing the new data regime will also be offered. Key lessons to be learned so far as the retention of criminality data is concerned will be identified and the chapter will conclude with comment as to how forthcoming developments might conceivably frame the future 'data problem' issue.

6.2 The Data Protection Act 1998

The DPA 1984 had made specific provision for criminal records; s.2(3) provided that the Secretary of State 'may by order modify or supplement the DPA 1984 to provide additional safeguards' for ensuring compliance with the Data Protection Principles.

No such safeguards were ever enacted. The Council of Europe, conscious that their 1981 Convention provided wide scope for police derogation, produced formal recommendations

on the control of data by the police.[1] These included provisions that police only collect data for the prevention of 'real danger' or 'the suppression of a specific criminal offence',[2] unless otherwise approved by specific legislation, that the data be 'accurate'[3] and limited to the data required to perform 'their lawful tasks' and that police data should only be used for police purposes.[4] The UK formally derogated from two of principles and adopted the others[5] but as the recommendations were non-binding,[6] the police and the Home Office were not legally obligated to follow them in any event.

The problems with the DPA 1984, many of which were foreseen by opponents prior to its enactment, began to become apparent. Despite an extensive publicity campaign by the Registrar,[7] levels of subject access were low, particularly those involving Government departments: cumulative charges for subject access to each registered executive databank could mean that the cost to an individual might reach some £900in total.[8] Perhaps unsurprisingly, the Home Office in 1988 received precisely 16 subject access requests.[9] Subject access requests to chief constables regarding criminal records were 'usually' granted, but some were denied on the basis of s.27 of the DPA 1984; a practice described by the Registrar as 'questionable'.[10]

It had been imagined that the Data Protection Registry would operate with a staff of twenty. By the end of 1984, the actual number of staff required was 'more than 40'.[11] Failure to register among businesses and organisations was rife: at 1994, only 180,000 of an estimated 3 million affected trading organisations had actually registered. The response of the Registrar was not particularly robust; in 1994, for example, the Registrar took action against 32 companies who did not register and, although fines were issued, the largest

[1] Council of Europe, Regulating the use of personal data in the police sector (Recommendation No. R(87) 15, 17 September 1987)
[2] Ibid, Principle 2.1
[3] Ibid, Principle 3.1
[4] Ibid, Principle 5.1
[5] Ibid, fn.1. It is *very* debatable as to whether the UK has actually fulfilled the recommendations, though that discussion is somewhat outwith this research. An examination of state fulfilment of the 1987 Recommendations is available at J. Cannataci and M. Caruana, 'Recommendation R (87) 15: Twenty-Five years down the line' (Council of Europe 25 September 2013)
[6] Explanatory Memorandum to Recommendation No. R (87) 15 (Council of Europe 17 September 1987), para.20
[7] HC Written Answers 17 February 1988, vol.127, col.618
[8] HC Deb 19 May 1989, vol.153, col.655
[9] Ibid
[10] M. Colvin, 'The Criminal Record and Information Systems in England and Wales' (1992) 6 International Yearbook of Law Computers and Technology 139, 146
[11] HC Deb 31 October 1984, vol.65, col. 1336

was £2000.[12] Even where companies were registered, the DPA 1984 conferred no power to the Registrar to investigate possible breaches unless a complaint was made to them.

By the start of the 1990s, the European Union were again taking an interest in data protection. The European Commission issued a proposal in September 1990[13] which aimed to provide 'a high level of protection via a community system of protection based on a set of complementary measures'.[14] This led to a five year 'harmonisation' process, using mainly amendments to the 1981 Convention and subsequent domestic laws[15] before the publication of a Directive[16] on October 24 1995 which laid down the new principles and rules to be implemented in member states. The police were again given fairly wide derogations from the general principles[17] – so much so that Haynes claimed that the Directive 'did not regulate the police'[18] – but, in fact, criminal convictions were expressly covered by Article 8(5), which provided that:

> Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

The UK, and other member states, were given three years to implement the directive into national law.[19] The Home Office, perhaps unsurprisingly, were unconvinced that new legislation was required[20], but Parliament nonetheless responded, after a lengthy process

[12] L. Curry, 'A stickler for our privacy: the new Data Protection Registrar is taking on banks', *The Independent* (London, 19 September 1994)
[13] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, Com (90) 314 SYN 287 and 288
[14] Ibid, Part II, para.9
[15] B. Hayes, 'A Failure to Regulate: Data Protection and Ethnic Profiling in the Police Sector in Europe' (2005) Open Society 32, 34
[16] Directive 95/46/EC of the European Parliament and the Council of Europe (24 October 1995)
[17] Ibid, Art.3(2)
[18] Above n.15
[19] Above n.16, Art.32(1)
[20] European Standing Committee B, 'Official Report', (December 1994) cc.3 – 22, col.3

of reports, committees and debates,[21] by bringing the Data Protection Bill[22] which would become the Data Protection Act 1998[23] ('the DPA 1998') on 16 July 1998.

The DPA 1998 did not, in truth, make significant changes to the legislative requirements so far as criminal records were concerned; indeed, the Registrar commented that the DPA 1998 generally 'is in substance very much the same as the current law: at least 80% of compliance flows from complying with the DPA 1984'.[24] It did repeal, entirely, the DPA 1984,[25] but it replaced many of its provisions with very similar or identical provisions.

One major change was that the DPA 1998 applied to computerised records[26] and 'those recorded as part of a relevant filing system'.[27] This meant that PHOENIX fell under the auspices of the DPA 1998 along with the microfiche collection of criminal records for those who had not yet 'come to notice': a Freedom of Information Request made in the course of this research revealed that this still amounts to just over one million unconverted microfiche records.[28]

The police were no longer 'data users' but instead 'data controllers': persons who (either alone or jointly) determine the purposes and manner in which the criminal record data is processed.[29] With the responsibility for updating PHOENIX taken from the NIB in 1995 and instead provided to individual police forces, this meant that each chief constable of the police forces contributing criminal records data to PHOENIX were joint data controllers. Any sub-contractors engaged by the police or the Home Office to work with the criminal records were 'data processors': any person (other than an employee) who processes data on behalf of the controller.[30] Those whose records were held on PHOENIX were still 'data subjects'.[31]

---

[21] For a summary of these, see E. Wood, 'Research Paper 98/48' (HC Library, 17 April 1998) 11 – 12
[22] The Data Protection Bill [HL] Bill 158 of 1997 – 98
[23] 1998, ch.29
[24] E. Frances, 'Data Protection Bill 2/98, Costs of Implementing the EU Data Protection Directive' (v.2.0, 29 January 1998)
[25] Ibid, Sch.16, Part I
[26] Ibid, Part I, s.1(1)(a)
[27] Ibid, Part I, s.1(1)(c)
[28] Home Office 'FOI Request – Collection of historic microfiche criminal records' (FOI case ref: 49433 *What Do They Know?*, 17 July 2018) <https://www.whatdotheyknow.com/request/collection_of_historic_microfich?nocache=incoming-1205670#incoming-1205670> accessed 20 May 2019
[29] Above n.23, s.1(1)
[30] Ibid
[31] Ibid

The DPA 1998 retained the operational rubric of protecting specified 'Data Protection Principles'. These, listed in Schedule 1,[32] are almost identical in nature (and largely in wording) to those in the DPA 1984, except that the second and third principles of the earlier Act had been merged into one principle[33] and that a new principle had been added to ensure that personal data was not transferred by a data controller to any other country who did not have comparable data protections.[34]

Criminal records were once more identified as 'sensitive personal data'.[35] This meant that especial provisions[36] applied for the processing of criminal records, though a number of exemptions,[37] such as where the data is required in connection with any legal proceedings,[38] the administration of justice[39] or where data is required for the exercise conferred under an enactment,[40] were again provided. The net result of the exemptions was, it is submitted, sufficient te effectively exempt the police criminal record collection on PHOENIX from the especial provisions.

In very similar provisions to the DPA 1984, those with criminal records were entitled to access them,[41] subject to the police right to exempt themselves if withholding the information helped prevent or detect crime[42] or in the prosecution or apprehension of offenders.[43] A new protection was provided to the police, which also provided an exemption to the first data protection principle in the same circumstances where they might avoid subject access.[44] Those who suffered damage or distress as a result of a data contravention were entitled to sue for damages[45] while a Court order might be sought to rectify, block, erase or destroy inaccurate data.[46]

[32] Ibid, Schedule 1, Part I, Principles 1 – 8
[33] Ibid, Schedule 1, Part I, Principle 2
[34] Ibid, Schedule 1, Part I, Principle 8
[35] Ibid, Part I, s.2(g)(h)
[36] Ibid, Schedule I, Part I, s.1(1)(a)
[37] Ibid, Schedule I, Part I, s.1(1)(b)
[38] Ibid, Schedule 3, s.6(a)
[39] Ibid, Schedule 3, s.7(1)(a)
[40] Ibid, Schedule 3, s.7(1)(b)
[41] Ibid, Part II, s.7
[42] Ibid, Part IV, s.29(1)(a)
[43] Ibid, Part IV, s.29(1)(b)
[44] Ibid and above n.41
[45] Ibid, Part II, s.13(1)(2)
[46] Ibid, Part II, s.14

The Registrar was given the new title of 'Data Protection Commissioner',[47] though this title was removed in 2000 and the new title of 'Information Commissioner' ('the Commissioner') instead conferred.[48] Data controllers were still obligated to report themselves to the Commissioner,[49] along with details of the personal data held by them[50] and the purposes for which it was held,[51] so that the Commissioner could compile a public register.[52]

The IC was expected to 'promote good practice' and 'promote observance' of the Act.[53] To this end, s/he could issue 'information notices' to compel the release of information as part of investigations into possible breaches of the DPA 1998,[54] as well as 'enforcement notices' similar to those permissible under the DPA 1984.[55] Failure to comply with an enforcement notice was an offence and a fine might be issued.[56] Disputes over decisions made by the IC were to be dealt with by recourse to the Data Protection Tribunal,[57] which in 2000 was renamed the 'Information Tribunal'.[58]

The question of whether the DPA 1998 applied to the PHOENIX collection of criminal records was definitively answered in the affirmative by the Court of Appeal in 2009.[59] The DPA 1998 applied to the police and the PHOENIX collection until it was almost entirely repealed by the Data Protection Act 2018 on 25 May 2018.[60]

As this research has shown, the chief constable data controllers responsible for the collation and maintenance of central criminal records under the auspices of the DPA 1984 appeared to commit a number of prima facie breaches of the provisions of the Act. The author will now consider whether similar charges might be brought against chief constables as regards the DPA 1998.

[47] Ibid, Part I, s.6(1)
[48] Per Part I, s.18 of the Freedom of Information Act 2000, Ch.36
[49] The Data Protection Act 1998, at Part III, s.18(1)
[50] Ibid, Part III, s.16(1)(c)
[51] Ibid, Part III, s.16(1)(d)
[52] Ibid, s.19(1)
[53] Ibid, Part VI, s.51(1)
[54] Ibid, Part V, s.43
[55] Ibid, Part V, s.40
[56] Ibid, Part V, s.47(1)
[57] Ibid, Part I, s.6(3)
[58] Per Part I, s.18(2) of the Freedom of Information Act 2000
[59] [2009] EWCA Civ 1079 [33]
[60] Per Schedule 19, Part I, s.44 of the Data Protection Act 2018, ch.12

6.3 Police compliance with the first data principle

According to Schedule 1, Part I of the DPA 1998, the first Data Principle required that 'personal data shall be processed fairly and lawfully'. The enabling provision which allows for the lawful collection of criminal records is s.27(4) of the Police and Criminal Evidence Act ('PACE 1984'), which provides that:

> The Secretary of State may by regulations make provision for recording in national police records convictions for such offences as are specified in the Regulations. 'Conviction' includes a caution and a reprimand or a warning'

This is supplemented by the Police Act 1997 (Criminal Records) Regulations 2002,[61] which provides that details of convictions, cautions, warnings and reprimands will be kept in 'central records'; i.e. the 'names database' on the PNC.[62] Where a conviction is obtained and recorded on PHOENIX via the various enabling mechanisms identified in chapter 3 of this research, it is so done 'lawfully'.[63] The same, however, cannot necessarily be said for arrests or cautions. An explanation of what is meant by this if offered below:

6.3.1 Unlawful arrests

A lawful arrest must either be carried out pursuant to a warrant[64] or under s.24 of the PACE 1984. It has become apparent, through recent litigation, that there are instances where the police conduct unlawful arrests. These might involve an situation where an arresting officer cannot make out the necessary legal grounds: in *Cumberbatch v the Crown Prosecution Service; Ali v Director of Public Prosecution*,[65] the Divisional Court held that an arrest is unlawful (and can be resisted by force) where none of the s.24 PACE 1984 grounds can be objectively made out.[66]

More commonplace is where the police place under arrest those who attend the police station voluntarily to 'help police with their enquiries'. Professor Michael Zander states

[61] 2002 S.I No.233
[62] Ibid, reg.9, as inserted by reg.2 of the Police Act 1997 (Criminal Records) Amendment Regulations 2007, S.I No.700
[63] Per schedule 2, s.2(3) and schedule 3, s.7(1)(a) of Data Protection Act 1998
[64] Per s.1(1)(b) of the Magistrates Courts Act 1980 and *Halsbury's Laws of England*, *Criminal Procedure* (2015), vol.27, para 144
[65] [2009] EWHC 3353 (Admin)
[66] Ibid [10]

that such practice is 'common and routine'.[67] He also believes that it is also 'unlawful and should stop'.[68] Instances of allegations made against teachers are often dealt with in this way, where the individual against whom the allegation is made attends the police station at a pre-arranged date and time and is duly arrested in the foyer by the investigating officer.[69] Where such arrests have not resulted in the accused being charged, it is possible to challenge (by judicial review) the lawfulness of the arrest.[70] However, the police response to a successful challenge is to add a note to the PNC to show that the arrest should not have taken place,[71] rather than to delete it.

In 2016 – 17, the police conducted 779,660 arrests.[72] In the same period, the Independent Police Complaints Commission ('the IPCC') received 2,589 allegations of unlawful/unnecessary arrest.[73] It is not known how many unlawful arrests were conducted which did not result in a complaint to the IPCC.

Similarly, although civil law provides redress to those who are wrongfully arrested,[74] it has been held that the arrestee is required to show that the arrest was *Wednesbury* unreasonable.[75] This is a high hurdle to overcome and suggests a considerable defence to police operational discretion. Moreover, an arrestee will ordinarily be denied access to legal aid to bring such a claim.[76] This does not necessarily mean that an arrestee is not given access to court to make a claim, but rather that they will not be able to do so with legal representation funded by the state.[77] According to the Ministry of Justice, this is because wrongful arrests are not among 'the most serious allegations of misuse of

[67] M. Zander, 'Arresting someone who is helping the police with their enquiries' (2010) 174 Criminal Law and Justice Weekly 309
[68] Ibid
[69] Ibid, 310
[70] *Jones v the Chief Constable of the West Midlands Police* (2006)
[71] *Wren v the Chief Constable of Northumbria Police* (2009) A summation is provided by Zander, above n.67
[72] J. Hargreaves, H. Husband and C. Linehan, 'Police powers and procedures, England and Wales, year ending 31 March 2017' (Home Office Statistical Bulletin 20/17, 26 October 2017) 10
[73] Independent Police Complaints Commission, 'Statistics for England and Wales 2016/17' (2017) 20
[74] See the dicta of Lord Keith in *Hill v the Chief Constable of West Yorkshire* [1989] AC 53, 59
[75] *Al Fayed and others v. Commissioner of Police of the Metropolis* [2004] EWCA Civ 1579
[76] Per Schedule 1, para.21 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012, as interpreted by the Court of Appeal in *R (on the application of Sisangia) v the Director of Legal Aid Casework* [2016] EWCA Civ 24
[77] Ibid [8]

power by public authorities'.[78] Quite how many potential litigants this discourages is not known, but the reasonable presumption must be that at least *some* are so discouraged.

It is not clear why the police retention of unlawful arrests on PHOENIX is not in contravention of the first DPA 1998 data protection principle. In circumstances where an unlawful arrest takes place but that there is no official determination that the arrest was unlawful, it is perhaps understandable that the data is retained. Where an arrest is demonstrably unlawful, however, it is conceivable that there is no lawful basis for the retention of data relating to that unlawful arrest on the PNC.

The applicable provisions in the DPA 1998 are complex. The police may claim that they are exempted from the first data principle because unlawful arrest data is required 'for the prevention or detection of crime' or for the 'apprehension and prosecution of offenders'.[79]. This may protect them in *some* unlawful arrest instances, but certainly not all. It is submitted that an arrest which is unlawful because the officers has no objective ground(s) to believe an offence has taken place must ordinarily involve arresting someone where no crime has occurred and where the arrestee is not an 'offender'. In such a circumstance, it is difficult to see how the s.29(1) DPA 1998 exemption would apply. Similarly, where an unlawful arrest takes place as part of an investigation into an allegation and that investigation finds that no offence took place, it is submitted that the exemption cannot apply. The issue is more nuanced than the blanket exemption might suggest.

Presuming that the exemptions are inapplicable, the first data principle will be satisfied provided that at least one of the conditions listed in Schedule 2 and one of those in Schedule 3 of the DPA 1998 are met. There are certain provisions in Schedule 2 which the police might invoke to legitimise the retention of unlawful arrest data. One provides that data may be retained if it has to be so done to fulfil a legal obligation of the data controller.[80] However, there are no legal provisions which mandate the collection of data relating to unlawful arrests.[81] It is not conceivable that the collection of unlawful arrest

[78] J. Hyde, 'Court overturns legal aid denial in wrongful arrest case' (*Law Society Gazette,* 13 November 2014) <https://www.lawgazette.co.uk/law/court-overturns-legal-aid-denial-in-wrongful-arrest-case/5045066.article> accessed 20 May 2019
[79] Above n.44
[80] Per Schedule 2, s.3 of the Data Protection Act 1998
[81] Strictly speaking, s.27(4) PACE and subsequent regulations do not mandate the statutory collection of *any* arrest data. There is nothing in that provision which relates to arrest data at all.

data is required 'for the administration of justice'.[82] Such information would not form part of any decision on bail, bad character admissibility, sentencing or probation.

The most plausible police defence is that the processing of unlawful arrest data is 'necessary for the purpose of the legitimate interests of the police'.[83] The ICO suggests that such a defence has three elements: the processing must be in pursuant of a legitimate interest, be necessary is respect of that interest and the individuals interests must not override the legitimate interest.[84] It is submitted that the police would struggle to meet these three requirements: it is difficult to envisage how the holding of unlawful arrest data is 'necessary' in pursuing the legitimate interest of crime prevention, detection and bringing offenders to justice for much the same reasons as stated in the immediately preceding paragraph.

In the absence of any Schedule 2 condition, the processing of such data is prima facie unfair and/or unlawful. It is submitted, therefore, that, where an arrest has taken place which is proven (either by subsequent police admission or by litigation) to be unlawful, then data relating to it was neither obtained nor processed lawfully and therefore should be deleted.

6.3.2 Unlawful cautions

It is not merely unlawful arrests which might give rise to a breach of the first data principle. There might also be concerns regarding cautions. There have long been anecdotal examples of people who accept a caution not because they are necessarily guilty of an offence but rather because the alternative – possible criminal prosecution – is too undesirable a risk.[85] Indeed, the Lord Chief Justice in 2011 wondered 'whether the convenience of avoiding the court process altogether may lead to an offender to admit to something for which he would have a defence'.[86] In *R (on the application of R) v Durham Constabulary and another,*[87] Baroness Hale recognised that there is always implicit, and occasionally explicit, 'pressure' to 'admit it and we'll [the police] will let you

[82] Per schedule 2, s.5(1)(a) of the Data Protection Act 1998
[83] Ibid, s.6(1)
[84] The Information Commissioner's Office, 'Guide to the Data Protection Regulation (GDPR)' (4 June 2018) 81
[85] A. Topping and B. Quinn; 'Charles Saatchi: accepting police caution was better than the alternative' *The Guardian* (London, 18 June 2013)
[86] Lord Judge, 'Summary Justice In and Out of Court' (John Harris Memorial Lecture, Draper's Hall, London, 7 July 2011) 15
[87] [2005] UKHL 21

off with a caution', particularly regarding juveniles.[88] Cautions issued in such circumstances may not be 'legitimate', in the sense that they may record criminality behaviour on the part of those not guilty of committing an offence, but they do not strictly breach the Home Office requirements on issuing cautions because the recipient nonetheless has made an 'admission' to the offence.

Of more concern are those circumstances where the Ministry of Justice guidelines are not followed in the issuing of a caution. This occurs largely because of a lack of a supervisory or oversight mechanism to review the issuing of cautions which are so done in private and 'on police territory'.[89] For example, although the current guidance expressly forbid the police from 'inducing [a suspect] to accept a simple caution in any way',[90] it has been claimed that police 'indications are often given before an interview that a caution is likely to be offered in the event of an admission'.[91] These might help an individual decide to make a damaging admission and in the hope of accept the proffered caution.

Such a claim was made in *R (on the application of Lee) v Chief Constable of Essex Police*,[92] where the investigating officer told the duty solicitor prior to interview and private consultation that the solicitor's client *could* (author's emphasis) be eligible for a caution due to the suspect's prior good character and the minor nature of the allegation.[93] Immediately after the interview ended, during which his client had admitted to the alleged offence, the solicitor told the interviewing officer that he had explained the ramifications of a caution to the suspect and that he would accept one.[94]

The Divisional Court rejected the application to quash the caution, claiming that the investigating officer 'did no more than inform [the duty solicitor] before his consultation with the Claimant that a caution might – and I emphasise the word "might" – be available…[the guidance] does not prohibit any mention of a possible caution by a police

[88] Ibid [36]
[89] J. C. Donaghue, 'Reforming the role of Magistrates: implications for summary justice in England and Wales' (1 November 2014) 77(6) Modern Law Review 928, 948
[90] Ministry of Justice, 'Simple Cautions for adult offenders' (13 April 2015) para.71
[91] P. Hynes and M. Elkins, 'Suggestions for reform to the police cautioning procedure' (2013) 12 Criminal Law Review 966
[92] [2012] EWHC (Admin) 283
[93] Ibid [7]
[94] Ibid [9]

officer at any stage before a confession is made'.[95] It is submitted that such a distinction must provide the police with an effective *carte blanche* to proffer blandishments to arrestee intended to encouraging admissions *en route* to the issuing of cautions, provided, of course, that the officer is sufficiently prudent as to not couch their proposition in too robust terms. It also risks the possibility of a solicitor misadvising a client to make an admission with a view to the offer of a caution which may, or may not, be forthcoming.

Such cautions, however obtained, will be retained on PHOENIX and are almost certainly not subject to data challenge where a judicial review as to the lawfulness of them generally has failed. In fact, the position at judicial review is that the oversight provided by the courts to the police discretion to issue cautions is limited indeed. In *Blackburn v Commissioner of the Police for the Metropolis,*[96] Lord Denning made clear that the police act independently of the Executive;[97] taken in that context, the Home Office/Ministry of Justice guidance produced on cautions is precisely that; guidance, and nothing more.[98] This helps to further explain the decision in *R (Lee)*, where the fact that the police did not even consider the most recent Home Office guidelines was not held to fatally undermine their decision to caution.[99]

A similar deference was shown in *R (on the application of Manser) v Metropolitan Police Commissioner.*[100] Here a caution was issued to Manser who, having returned to the scene of an unprovoked attack on her and seeing one of her assailants pinned to the floor by security staff, duly delivered a kick to her face.[101] After being arrested for causing grievous bodily harm with intent,[102] she was told at her subsequent police interview that her kick had caused the woman to 'lose a front tooth, a split lip and a broken nose'.[103] In fact, she had not broken the woman's nose at all and the police failed, despite repeated requests, to provide any evidence to show such an injury was caused.[104]

[95] Ibid [19]
[96] [1968] 2 QB 118
[97] Ibid, 136 b – c
[98] *R (on the application of Stratton) v Chief Constable of Thames Valley Police* [2013] EWHC 1561 [40]
[99] Above n.92 [31]
[100] [2015] EWHC 3642 (Admin)
[101] Ibid [9][10]
[102] Contrary to s.18 of the Offences Against the Person Act 1861
[103] Above n.100 [13]
[104] Ibid [33]

On the basis of the representation of the injuries caused and viewing the CCTV which showed her deliver the kick, Manser nonetheless made an admission during interview and accepted a caution for assault occasioning actual bodily harm.[105] She later contested the caution as being unlawfully issued on the basis of the inaccurate representation and also on the basis that she only accepted the caution for ABH because she did not wish to risk contesting a prosecution on the charge of GBH. The Administrative Court held that there were no grounds to quash the caution.[106] Although the police had not strictly followed the applicable guidelines, their failure was not 'a clear breach of the guidelines' sufficient to necessitate the quashing of the caution.[107] Moreover, the offer of a caution for ABH, rather than a prosecution for GBH, was not to be construed as an 'inducement' because 'a caution can be properly offered for a lesser offence even if the police are considering prosecuting for a more serious offence'.[108]

Another example of the courts' unwillingness to intervene in the absence of a 'clear breach of guidelines' was provided in *R (on the application of Mondelly) v Commissioner of Police for the Metropolis*,[109] where the majority found that, despite the creation of a new statutory regime and applicable guidelines aimed principally at dealing informally with (or at least by not generally arresting) those caught in possession of cannabis, the applicant could not demonstrate that there had been a 'clear breach of guidelines'[110] when he was arrested at home by police who had been investigating a burglary and knocked on his door by mistake.[111] Walker J, however, disagreed, and said he would have quashed the conviction because 'the caution issued to Mr. Mondelly clearly contravened the Commissioner's policy on the simple possession of cannabis and for no good reason'.[112]

This line of authority illustrates starkly the very subjective nature of the decision-making process which informs the issue of cautions and also the very subjective nature of the analysis of what constitutes 'a clear breach of guidelines', so far as judicial oversight is concerned. They also demonstrate the clear judicial reluctance to interfere in the

[105] Ibid [20]
[106] Ibid [39]
[107] Ibid [34]
[108] Ibid [37]
[109] [2006] EWHC 2370
[110] Ibid [50]
[111] Ibid [1]
[112] Ibid [65]

decision-maker's subjective discretion where cautions are issued. However, examples of cautions being quashed can be found, and generally start from the decision in *R v Commissioner of Police of the Metropolis ex parte* P,[113] where the Divisional Court quashed a caution issued to a twelve-year-old boy arrested on suspicion of shop theft. This was ordered because the the boy had both been misled as to the necessary legal elements of the offence of shop-theft and there was no evidence at interview of any clear or reliable admission of guilt.[114]

Simon Brown LJ confirmed that 'the Court can properly intervene if a caution is administered in clear breach of the guidelines'[115] but he warned that the court had a discretion to intervene in such circumstances and not more[116] and that there was no intention 'to offer any sort of general encouragement to those cautioned to challenge the legality of their caution'.[117]

Soon after, in *R v Commissioner of Police of the Metropolis, ex parte Thompson*[118] the Divisional Court quashed a caution issued to a man in respect of a public order offence[119] when he began shouting abuse at police officers who (wrongly) stopped him for driving whilst under the influence of alcohol.[120] This was because the cautioning procedure used by the defendant police force informed him that being cautioned would remove the possibility of a court prosecution and ensure that he would not receive a criminal record[121] before asking if they admitted the offence, effectively inducing him to confess.[122] The general position of the law regarding the challenge of cautions issued was stated as being that:

> Judicial review is available as a remedy in respect of a caution; that this court will not invariably interfere, even in the case of a clear breach of the guidelines relating to the administration of cautions, as the availability of a remedy is a matter for the discretion of the court; that police officers "must enjoy a wide margin of appreciation

[113] (1995) 160 JP 367
[114] Ibid, 367 – 8
[115] Ibid, 371
[116] Ibid
[117] Ibid, 375
[118] [1997] 1 WLR 1519
[119] Contrary to s.5 of the Public Order Act 1986
[120] Above n.118, 1521
[121] Ibid,1524
[122] Ibid, 1525

> as to the nature of the case and whether the preconditions for a caution are satisfied;" and that it will be a rare case where a person who has been cautioned will succeed in showing that the decision was fatally flawed.[123]

Although clearly intended to limit applications to quash cautions only to very narrowly prescribed, fact-specific circumstances, the decisions in *P* and *Thompson* have generated a reasonably lengthy line of subsequent litigation. In *Abraham v Commissioner of the Police of the Metropolis*[124] a black woman told a black man being arrested on the street that she 'hope[d] to see you alive again' as she walked past with her two-year-old child. The police officer responded by following her down the street, manhandling her and arresting her for assault.[125] Abraham accepted a police caution on the advice of the duty solicitor, fully intending to get out of the police station as quickly as possible and bring an action for civil damages.[126] The Court of Appeal, overturning the decision of the single judge to strike out her claim, agreed that 'having been brought to the police station under a false pretext'[127] and no doubt concerned as to her son's welfare, she made an admission 'to an account of events which both she and P.C Cook knew to be false'.[128] Such an admission was not a true admission of guilt but rather one 'caused by, or at least contributed to' by the unlawful arrest and false recounting of events.[129]

In *R (on the application of Wyman) v Chief Constable of Hampshire Constabulary*[130] a student cautioned for sexual assault[131] after a complaint was made by a woman he had 'provocatively' danced with in a nightclub. Silber J found that the alleged 'admissions' made during the police interview were not 'clear or reliable' enough to show that he admitted that he did not have consent for touching the complainants bottom,[132] nor that his touching was 'sexual'[133] and so the caution should be quashed.[134]

---

[123] Above n.115
[124] [2001] 1 WLR 1257
[125] Ibid, 1259
[126] Ibid
[127] Ibid, 1262
[128] Ibid, 1263
[129] Ibid
[130] [2006] EWHC 1904 (Admin)
[131] Per s.3 of the Sexual Offences Act 2003
[132] Above n.130 [22]
[133] Ibid [23b]
[134] Ibid [24]

Another caution was quashed in *Caetano v Commissioner of Police of the Metropolis.*[135] Here, the police arrested a woman whose boyfriend returned home at 1am, drunk and proclaiming to have performed oral sex with another woman because 'he could do whatever he wanted', resulting in her slapping him twice. He then responded by putting his knee into her back and strangling her.[136] The police, taking the view that as she struck first, she was the aggressor,[137] duly arrested and interviewed Caetano before producing a summary of her interview for the custody officer which (falsely) claimed that she admitted to striking her boyfriend 'in the face several times' and that there was no bruising evident to substantiate the strangulation claims.[138] In fact, Caetano had offered during interview to show the officers photographs on her mobile showing bruising, but they declined.[139] On the basis of the summary, Caetano was cautioned by the custody officer. The caution was ultimately quashed because the decision maker had (based on the inaccurate interview summary) incorrectly categorised the alleged offence as 'domestic violence', when the reality was very different and something sufficiently minor that there would have been no public interest in issuing a caution.[140]

R (on the application of Stratton) v Chief Constable of Thames Valley Police[141] a caution was issued to a woman after she admitted to throwing a bottle at a woman who had poured a drink over her at a public house.[142] The claimant made an admission to common assault during interview but afterwards asked if the arrest would have any impact on her work as a children's nanny. She was told it would not.[143] Anxious to go home, she then signed what she believed to be 'a sign out form',[144] but was in fact a caution on a prescribed form, which stated that the caution might be used against her in any future legal proceedings[145] but which made no mention to any other potential adverse use of the caution. This, according to the Divisional Court, meant that she considered the form merely 'a formality that would enable her to leave the station…she probably thought no more about it'.[146] The failure of the police to intimate to an

[135] (2013) 177 JP 314
[136] Ibid [4]
[137] Ibid [9]
[138] Ibid [11][12]
[139] Ibid [8]
[140] Ibid [44]
[141] [2013] EWHC 1561
[142] Ibid [7]
[143] Ibid [12]
[144] Above n.142
[145] Ibid [8]
[146] Ibid [52]

unrepresented individual who works with children the potentially serious ramifications of being cautioned meant that she could not be said to give informed consent to the caution, and so the caution was quashed.[147]

What this relatively small sample of the unlawful caution litigation shows is that the concerns regarding the lawfulness of cautions issued by police, in the privacy of the station without immediate independent oversight, are at least partially justified and perhaps, it is submitted, in fact well-founded. Even in the small sample provided, it is evident that the police have issued cautions where there have been no good public policy reasons to do so, where there have not been reliable admissions to essential legal elements of the alleged offence, where arrests are affected on wholly inflated grounds, where the cautioning officer is provided with misrepresentations as to the material facts of the alleged offence by investigating officers, where officers have (deliberately or otherwise) misled the recipient as to the possible consequences of the caution and where the police have adopted procedures which facilitate an admission after the prospect of a caution has induced the suspect to confess.

The 'court approach' first offered in *Thompson* means that 'the practical issue of what was in fact happening in police stations was never properly considered'.[148] Some people may be accepting cautions not because they actually committed an offence but because they would rather deal with the matter privately than deal with the potentially far-reaching consequences of possible media reporting on their prosecution.[149] Moreover, the custody suite at the police station is a highly pressurised and frightening environment and it is submitted that the potential for poor decisions to be taken there, particularly by juveniles, those inexperienced in the custody process or the unrepresented, is obvious. Advice as to the caution and its ramifications provided by police might be wrong, either deliberately or inadvertently, because the police are not experts in criminal, employment, data protection, human rights or immigration law; just some of the areas potentially touched upon by the imposition of a police caution. Even where the suspect is represented, as in *Caetano*, the pressure on the individual may be such that the desire to leave custody is such that even an intelligent suspect who has taken legal advice may simply accept a caution which should not have been issued.

[147] Ibid [54]
[148] Above n.91, 969
[149] M. Elkins, 'Adult Defendant anonymity in Criminal Proceedings' (2016) 180 Criminal Law and Justice Weekly 387

Quite simply, it is not possible to know precisely how many people truly do accept a caution because they just want to go home. What is known is that, so far as most detainees are concerned, how quickly they will be released from custody is 'very often the primary concern'.[150] The temptation to 'seize it [a caution] as a way of securing immediate release from an unpleasant situation' is obvious.[151] Similarly, how many cautions have been issued in circumstances analogous to those raised in litigation is not, and likely never will, be known, but it is submitted that the litigated cases must merely represent the tip of an iceberg, and if even if only 1% of cautions are unlawfully issued, then between 2001 and 2013 alone this means that over 30,000 unlawful cautions were issued.[152]

Where a caution has been 'unlawfully' issued but not challenged, it will be nonetheless recorded onto PHOENIX as a 'factual' part of an individual's criminal record. Where the 'unlawful' conviction is challenged and successfully quashed, the record *might* be expunged from PHOENIX; it appears that the question of whether it is so done depends on the nature of the order made by the court at the conclusion of the successful challenge. In *P*, the court ordered that the conviction be quashed and also required that 'it be expunged from the police's records'.[153]

None of the other cases referred to in this chapter refer to such an order with the exception of *Wyman*, which provides an interesting insight into the issue of whether the quashing of a caution means that record of it is expunged. Here, upon confirmation that the caution would be quashed, the judge invited submissions as to the wording of the subsequent order. Counsel for the claimant asked that the conviction be quashed, costs be awarded in the case and 'that the Claimant then sought an order that all records relating to the caution be destroyed and that the said caution be expunged from all relevant records'.[154] This was not contested by the police but instead they advanced two issues 'which might assist the court'.

[150] Above n.91, 971
[151] Ibid
[152] Ibid, 966. The article cited at n.91 provides an extensive, practitioner's view as to the reality of the cautioning process at the police station and the inherent problems with it.
[153] Above n.113, 375 F
[154] Above n.130 [25][26]

Firstly, if the caution was to be quashed, the record should be retained because the chief constable may take the view that a prosecution should be brought instead.[155] The judge, while refusing to apply such a consideration in the instant case,[156] did not dismiss such an idea as unlawful and, therefore, it is perhaps worth noting that there is an inherent risk that a person who successfully seeks to quash a caution as unlawfully issued might render himself liable to prosecution instead. Moreover, it will be recalled that s.29(1) of the DPA 1998 provides an exemption to the requirement that data be collected lawfully if it is required 'for the prosecution of offenders'. The invocation of that defence in circumstances such as these might conceivably justify an extremely lengthy retention on PHOENIX; there is generally no time limitation on the bringing of a criminal matter and the threat of a potential prosecution therefore may hang, as a Sword of Damocles, for very many years.

The second issue was that the retention of the record might be required to enable the Defendant to resist any civil action subsequently brought by the Claimant.[157] This might have given rise to a police defence that such data is obtained and processed lawfully and fairly as it is necessary 'for the administration of justice'.[158] Such a position was, however, rejected by the judge, who simply provided that 'the existence of the caution is a matter recorded in this judgment'[159] and, indeed, the judge duly set out the wording of it in the appendix. In doing so, he effectively repudiated the necessity of retaining the record purely for litigation purposes.

It is submitted that data obtained as part of the process of issuing 'unlawful' cautions is *prima facie* unfair and/or unlawful and should be expunged. This is particularly so where either the police accept, or a court orders, that the caution is 'unlawful' and must be expunged. It should not be required that the claimant in such cases ask that the applicable PHOENIX data be deleted. This should be done as a matter of course if it is not so being done. Attempts by the police to defend the collection and retention of such data must fail, it is submitted, on the same grounds that a defence to collecting unlawful arrest data must fail. The ICO has not issued any enforcement notices in relation to data

[155] Ibid [27]
[156] Ibid
[157] Ibid [28]
[158] Per Schedule 2 of the Data Protection Act 1998.
[159] Above n.157

retained relating to unlawfully issued cautions. It is submitted that he may wish to consider the matter.

6.4 Police compliance with the fourth Data Principle

Accord to Schedule1, Part I of the DPA 1998, the fourth Data Principle requires that personal data shall be 'accurate and, where necessary, up-to-date'. Problems with the accuracy of the criminal record data had persisted for over two decades and had resulted in a Police Research Group making several key recommendations to improve the data quality. A subsequent ACPO audit sought to examine compliance with the PRG recommendations. They found that 'many forces had not implemented them, or even had plans to do so'.[160] ACPO were sufficiently concerned that they issued an 'ACPO Compliance Strategy for the Police National Computer',[161] which recognised that failings in leadership and training meant that many forces viewed 'national systems primarily as…functions of record keeping',[162] rather than investigative tools, so that 'a significant number of forces do not achieve the present standards'.[163] It imposed a number of key indicators, including that arrests and charges be entered 'in full' onto the PNC inside five days, police bail details added within 24 hours and court disposals within 72 hours of coming to police notice.[164]

The situation did not immediately improve. In 2000, Her Majesty's Inspectorate of Constabulary conducted an audit into the PHOENIX data. It's findings would have been quite shocking, were they not entirely predictable. The audit team found that none of the inspected forces had put in place an implementation plan regarding the PRG recommendations[165] and that the level of understanding regarding PHOENIX's investigative capabilities remained very low; one detective superintendent was entirely unaware as to how to use QUEST to search the PHOENIX data.[166] It also found that many forces were trying to meet timeliness targets by quickly adding 'skeleton' records – sufficient to generate a new PHOENIX record but no more – which never progressed to full records because their existed no mechanism to check that these were populated

[160] K. Povey, 'On the record; thematic inspection report on police crime recording, the police national computer and Phoenix Intelligence System data quality' (HMIC July 2000) 83
[161] R. Earland, 'Compliance Strategy for the Police National Computer' (ACPO 16 February 2000)
[162] Ibid, 2 – 3
[163] Ibid, 9
[164] Ibid
[165] Above n.160, 85
[166] Ibid, 93

later.[167] Inspectors asked for sight of the 'PHOENIX Source Documents' ('PSDs')[168] which were to be input by PHOENIX staff on the day of inspection to examine when the paperwork was initially completed. They found that some of the documents had been drafted 278 days earlier; a situation described by inspectors as 'unacceptable'.[169]

Moreover, the inspectors found all manner of inaccuracies and omissions in the data itself. Postcodes, a 'key search criterion' in QUEST, were missing in more than half of the records added by six of the ten inspected forces.[170] Inspections of one force showed that none of the PSDs to be input to PHOENIX included any descriptive details whatsoever, while another was found to have submitted incomplete PSDs in 37 of 40 inspected cases.[171] One force had included adequate *modus operandi* data on precisely four records, against a total recorded crime figure of 140,874 offences, in the year prior to the inspection.[172] Remarkably, omissions on the PSD led meant that some inputting staff 'would sometimes guess the details'.[173] Dates of birth were found to be wrongly recorded,[174] a man with a distinctive tattoo had evaded capture for some time because the 'tattoo' filed on his last PSD was left blank,[175] heights, eye colours and builds were wrongly recorded or missing.[176]

The overall picture was, according to the inspectors, 'totally unacceptable'.[177] That is perhaps being generous; in truth, the situation appeared to be wholly shambolic. The police tried to assuage fears by claiming that most of the problems lay 'in the main with personal descriptive detail', rather than convictions.[178] That may be so, but it does not explain why the delay in adding arrest details onto PHOENIX varied from five days (in the best forces) to 92 days (in the worst), or why the delay in inputting court disposals onto PHOENIX once received by police varied from 15 to 354 days.[179] Forces claimed they had

[167] Ibid, 126
[168] These are forms completed by officers containing the necessary information for support staff to input data onto PHOENIX. See above n.160, 133
[169] Above n.160, 134
[170] Ibid, 130
[171] Ibid, 138
[172] Ibid, 131
[173] Ibid, 141
[174] Ibid, 140
[175] Above n.172
[176] Ibid at 141 – 2
[177] Ibid at 142
[178] Select Committee on Home Affairs, *Criminal Records Bureau* (HC 227, 2000–01, 2-I) appendix 8, para. 2.2
[179] Ibid [28]

no recourse to check the accuracy of the data provided by court staff; unless reports contained an 'obvious error', data was simply input as received.[180]

In 2001, the Home Office sent HMIC in once more to inspect police responses to the problem. The situation remained extremely grave. The target time for the input of 90% of arrest data being input to PHOENIX was one day. The national average at March 2001 was 'a totally unacceptable' 55 days.[181] Moreover, the backlog of case disposals which had not been updated on PHOENIX was absolutely enormous; it was calculated that some 216,891 cases were 'overdue for finalisation' (i.e. had concluded months previously but the result not been added to PHOENIX).[182] This backlog meant that police were permanently chasing their tails and ACPO made it a priority target to 'validate' every one of the outstanding disposals inside twelve months.[183] After six months, the average time taken to record arrest data had fallen to 'only' 37 days.[184] Better progress was made on the backlog, with 50% cleared in six months, but progress was being hampered by the increasing awareness that 'some chief officers had simply not considered the issue to be a sufficiently high priority to warrant the effort required'.[185] It was only after a second round of inspections in April 2002, and serious cajoling of some chief officers by the Inspectorate, that something approaching an acceptable state of affairs was reached, with average arrest data input down to 'only' 16 days,[186] while the outstanding case backlog was down to 64,503, or 1,343 per force.[187]

It is submitted that the long-standing problems with accuracy of the PHOENIX collection of criminal records constituted a *prima facie* breach of the fourth DPA 1998 data principle. The police were certainly concerned that they were at risk of being in formally sanctioned by the ICO; ACPO's compliance strategy conceded in April 2000 that 'at present the service may not meet the Registrar's standards on relevance, accuracy and timeliness' and warned both that 'if our systems are defective, the Data Protection Act will increase

[180] Ibid, appendix 8, paragraph 2.4
[181] Home Office, 'Police National Computer: Data Quality and Timeliness – Report by HM Inspectorate of Constabulary' (HMIC 2001) 14
[182] Ibid, 15
[183] Ibid, 16
[184] Ibid, 19
[185] Ibid, 21
[186] Home Office, 'Police National Computer: Data Quality and Timeliness – Second Report on the Inspection by HM Inspectorate of Constabulary' (HMIC 2002) 21
[187] Ibid, 24

the likelihood of litigation against the service' and that 'given the Registrar's considerable enforcement powers, compliance is essential'.[188]

The Registrar (or the Information Commissioner, as she became in 2000) was fully *au fait* with the situation. She later told a Home Affairs Committee that her office had 'taken a keen interest in the quality and extent of criminal conviction data held on the PNC'[189] and indeed she had been sent a copy of the PRG Report which initially highlighted the deteriorated quality of the criminality data.[190] In response to growing concerns regarding the PHOENIX data, the assistant data commissioner issued a thinly veiled threat of enforcement action, telling *Computer Weekly* that 'we would not take a different stance to breaches by the police than we would a commercial organisation. It will be in the police's best interests to make sure it's house is in order'.[191] The poverty of the PHOENIX data was highlighted in the Information Commissioner's annual report in 2001, where she provided that 'substantial improvements' were required.[192]

Her response to the PGR research was to initiate meetings with ACPO and the Home Office which fed into the ACPO Compliance Strategy.[193] Her response to the 'alarming'[194] and 'unacceptable'[195] state of affairs highlighted in the HMIC inspection report in 2000 was to initiate more discussions with ACPO and the Home Office, rather than issue enforcement notices.[196] The Commissioner justified this on the basis that 'it has always been the Commissioner's approach to seek compliance initially through agreement rather than formal enforcement action'[197] though, if remedial action was not taken within a 'reasonable time, consideration would be given as to whether formal enforcement action would be taken'.[198]

This author submits that the Commissioner's approach was not correct, and she should instead have issued enforcement notices against chief officers, particularly once it became

[188] Above n.167, 1
[189] Above n.178, appendix 7, para.3.1
[190] Ibid
[191] M. Simons, 'Errors rife in police data file' *Computer Weekly* (London, April 2000)
[192] R. Huseyin, 'The Commissioner's Annual Report' (1 September 2001) 1(8) Privacy and Data Protection 1, 3
[193] Above n.178, appendix 7, para. 4.1
[194] Ibid, para.5.1
[195] Ibid, para. 5.2
[196] Above n.194
[197] Ibid, para.7.1
[198] Ibid

clear in 2001 that some were continuing to take a belligerent, almost recalcitrant, attitude towards rectifying the deficiencies in the data. Her claim that 'initial' cooperative action is best might well be true, but the problem had been evidence for some fifteen years or more – it is not clear just how many years the Commissioner considers to be part of an 'initial' phase of arrangement, but it is submitted that fifteen or more might not reasonably qualify. It is further submitted that, by failing to act decisively, the Commissioner facilitated the breach and encouraged it to continue; recalcitrant chief officers might naturally find more encouragement to be so once it became apparent that enforcement action was not forthcoming.

The Commissioner may argue that her approach has achieved the desired affect and facilitated improvements, but it is submitted that an analysis of subsequent problems which emerged through the disclosure of records for vetting purposes showed that inaccuracies persisted. In 2003, the government boasted that it had processed around 1,000,000 checks and had an error rate of 'just' 1%; one MP noted pointedly that this 'means that 10,000 people were wrongly assessed'.[199] In April 2004, an answer to a written Parliamentary question revealed that in the preceding twelve months, some 193 applicants were wrongly labelled as offenders.[200]

Academic criticism began to surface; in 2005, for example, Jan Miller reported that around one-third of employers had complained that checks provided inaccurate information.[201] In April 2006 it was revealed in the Commons that some 1,472 mistakes had been made since March 2004.[202] The BBC soon after reported that once such incident saw one woman mistakenly labelled a convicted shoplifter. A further question in Parliament in June 2006 showed that the total number of complaints upheld relating to mistakes made from 2003 to the end of the 2005/6 financial year to be 2,273.[203] In 2007, the media reported that one woman had lost two jobs and was currently suspended from a third after 'her' criminal record continued to show, incorrectly, that she had drink-driving and drug-related convictions.[204] In 2008 it was reported that 680 innocent people had been implicated in

[199] HC Deb 30 April 2003, c.114WH at c.112WH
[200] HC Deb 19 April 2004, c.92w
[201] J. Miller, 'News – Long wait to check staff criminal records' (12 August 2005) 155 New Law Journal 1230
[202] HC Deb 11 May 2006, c.511w
[203] HC Deb 28 June, 2006 c.506W
[204] 'Women in wrong identity blinder' *The BBC* (London, 25 June 2007)

criminal offences;[205] one shadow minister duly noted that: 'nearly 700 mistakes that could ruin people's lives is 700 too many'.[206]

In December 2008 it emerged that the figures released regarding errors to date were, in fact, somewhat selective, and in fact the number of disputes which had resulted in an amended certificate were significantly higher than previously claimed; the total number of disputes regarding the accuracy of information provided from criminal records which turned out to be wrong was (from 2003) actually 12,255.[207] There appeared to be no resolution to the now perennial problem of inaccurate records. In 2009, 1,570 erroneous checks either showed convictions against applicants who had none or which declared a person free from convictions when they had in fact been so convicted.[208] In 2012, a Freedom of Information (FOI) request revealed that the total number of disputes raised against checks where the raw data on PHOENIX was simply wrong had reached 'more than 3,500'.[209]

The Information Commissioner's response to this continued problem is to do nothing. A Freedom of Information Request sent by this author to the ICO confirmed that the Commissioner has still issued no enforcement notices against any police force in respect of data breaches concerning the accuracy of the PHOENIX record.[210] It is submitted that the Commissioner's continued inaction is inexcusable and has done little more than facilitate ongoing data protection breaches which now stretch beyond three decades and, for reasons exculpated in the remaining chapters, potentially have a significant detrimental impact on the lives of individuals affected.

---

[205] C. Hope, 'Hundreds of innocent people 'wrongly branded criminals' by CRB checks' *The Telegraph* (London, 4 July 2008)
[206] Ibid
[207] HC Deb 6 November 2008, c.636W
[208] 'UK criminal vetting errors double' *The BBC* (London, 3 August 2009)
[209] T. Whitehead, 'Thousands wrongly labelled as criminals' *The Telegraph* (London, 2 February 2012)
[210] The Information Commissioner, 'FOI Request. Data relating to enforcement notices issued to police forces in respect of the nominal index of the PNC' (Case Ref No. IRQ0772426, *What Do They Know?* 1 August 2018) <https://www.whatdotheyknow.com/request/data_relating_to_enforcement_not#describe_state_form_1> accessed 1 August 2018

6.5 Police compliance with the seventh Data Principle

According to Schedule 1, Part 1 of the DPA 1998, the seventh Data Principle required that 'appropriate technical measures be taken against unauthorised or unlawful processing of personal data'. The problem of unlawful access by police officers to data, which have occurred since the 1980s, show no signs of being properly addressed, or, at least, instances of unauthorised use and misuse continue to surface. In *R v Rees*[211] a former detective inspector at Warwickshire Constabulary who had set up a private investigation agency was able to persuade a former colleague, a serving detective sergeant, to provide him with details contained in PHOENIX on some 29 occasions.[212] Both were imprisoned, despite an elaborate attempt by the more senior former officer to claim that no offence had been committed because criminal record information was not 'confidential' as criminal convictions were a matter of public record; the Court of Appeal describing the use of the word 'confidential' in this context as 'otiose' and meaning nothing more than that the data is restricted to the police for policing purposes.[213] In the course of the trial in this case, it emerged that the same force had recently dismissed another officer for similar PNC breaches.[214]

At largely the same time, in *R v Keyte*[215] another serving police officer was jailed after releasing PHOENIX information to several former police officers who had instigated private investigating agencies in return for small payments.[216] The Court of Appeal reiterated that:

> The integrity of the Police National Computer is of absolutely vital importance and it goes without saying that the public must have faith and confidence in it and a belief that private information relating to them will not be released by police officers for ulterior motives.[217]

The use of PHOENIX data by private investigators was concerning enough, but it seemed that unauthorised or unlawful processing had spread to even more nefarious

[211] [2000] ALL ER (D) 1481
[212] Ibid [5]
[213] Ibid [22]
[214] Ibid [28]
[215] [1998] 2 Cr. App. R.(S.) 165
[216] Ibid, 166
[217] Ibid

circumstances. In *R v Nazir*[218] an experienced officer persuaded a trainee in his charge to 'toss a coin' for possession of a PND issued to a friend of the experienced officer.[219] When the coin toss was lost, the new recruit reported the incident, after which the officer freely admitted that his intention was to destroy it before it appeared on PHOENIX.[220] The officer in question was imprisoned for one month.[221] It seemed that some officers were even prepared to use information on PHOENIX to help facilitate criminality. In *R v Gellion*,[222] an intelligence officer saw information on the PNC which indicated that a family friend (and known criminal) was to be subject to police surveillance. The officer warned the criminal that this was to happen and evidence was destroyed as a result.[223] It took a police 'sting' operation to trap the officer, who was eventually convicted of misconduct in public office and jailed.[224]

The case of *R v Hardy*[225] provided an example of an even more remarkable misuse of PHOENIX data. H, an experienced officer, was a long-standing friend of J; a known offender with a history of offences, including some involving serious violence.[226] Once this association was discovered and it was found that H had looked up J on PHOENIX, H was formally reprimanded by his employer and warned to sever all ties with J.[227] He did not do so. Instead, in 2006 J asked H if he 'knew' two men who J suspected was responsible for thefts from J's partner's public house. Very shortly afterwards, J was violently attacked by a different man, W.[228] H duly looked up the two men J thought responsible for the theft, and W, on PHOENIX.[229] J told H that he thought W would be arrested soon and so he needed to 'get him quick'. J duly printed out the PHOENIX records of all these men and got his partner to copy them and hand them over to J, to ensure no fingerprints would link H to the printout. Unfortunately for all concerned, the police had placed both H and J under covert surveillance and both were arrested as the information was handed over.[230] When interrogated, H defended his actions by claiming that the two men suspected of the

[218] [2003] EWCA Crim 901
[219] Ibid [2]
[220] Ibid [3]
[221] Ibid [6]
[222] [2006] EWCA Crim 281
[223] Ibid [2]
[224] Ibid [5]
[225] [2007] EWCA Crim 760
[226] Ibid [5]
[227] Ibid [7]
[228] Ibid [11]
[229] Ibid [12]
[230] Ibid [14]

theft were ‘known heroin addicts who were responsible for a lot of crime in the area’ and that the police would not have dealt with the violent attack by W because J was a known offender with a history of violence himself. In short, he felt that ‘justice needed to be done’ and that the police and the criminal justice system would not facilitate this.[231]

It seems that the misuse of criminal records data extended beyond even individual police officers deciding to bypass the criminal justice system in favour of allowing habitual and violent offenders to ‘punish’ criminals instead. An article in *The Guardian* in 2011 claimed that police ‘Operation Reproof’ had uncovered a ‘nationwide network of private detectives’ who were being fed information from the PNC by corrupt police officers on, among others, prominent Labour party politicians in 2005, including a criminal record check on Gordon Brown. It was further claimed that these were being requested by journalists under instruction from Rebekah Brookes, then editor of the now defunct and disgraced *News of the World.* The report concluded that it was ruled by a judge that bringing a prosecution against those involved would involve disproportionate costs in such a ‘trivial matter’, so the police investigation was brought to a close.[232] It is not immediately evident why an unlawful investigation into the background of the then Chancellor of the Exchequer involving the illegal release of PNC data by serving police officers at the request of investigators acting for an editor of a national newspapers might reasonably be considered ‘trivial’.

The media continued to report on higher profile examples of illegal access to the PNC. In 2007 a group of serving and former police officers were convicted of various offences relating to the PNC, including (the by now almost routine) dissemination of information on criminal records to private investigators.[233] Mark Turner, another serving police officer, was jailed in 2010 after a trial showed he was passing criminal records to his criminal associates.[234] Turner later came to prominence once more in 2015 when he was jailed for his part in a drug dealing gang.[235] A 2011 article claimed that ‘over 200 staff’ in the

[231] Ibid [17]
[232] D. Leigh and N. Davies, ‘Evidence of illegal data checks on Gordon Brown buried by 2005 ruling’, *The Guardian* (London, 11 July 2011)
[233] ‘Former police private eyes jailed’ *The BBC* (London, 10 October 2007)
[234] ‘Court of Appeal overturns sentence on West Midlands police officer and imposes prison term’ *The Birmingham Post* (Birmingham, 16 October 2009)
[235] ‘Ex-West Midlands Police officer jailed in drugs charge’ *The BBC* (London, 24 April 2015)

Metropolitan Police had been disciplined for unlawful access to the PNC in the preceding ten years. Over half of the incidents had been recorded in the previous three years.[236]

A detailed analysis of the minutiae of these cases is not required. Rather, these demonstrate once more that the problem of unauthorised and unlawful use of criminal records data continues long after it was first publicised as a serious problem by James Rule in 1970. A Freedom of Information request by this author in the preparation of this research has confirmed that the Information Commission has not issued any enforcement notices against any chief officers relating to unauthorised or illegal access or processing of criminal records.[237] It is not clear at all why this is so. It must be presumed that the Commissioner feels that that chief officers cannot be blamed for 'isolated' actions of 'rogue' officers and that the preventative and responsive measures taken by chief officers generally provide a reasonable defence to any data protection breach.

There is perhaps a measure of truth to such a submission. It is clear from the above-stated cases, for many years, logs have been taken of PNC access and that forces conduct 'spot-checks' on these to monitor use.[238] These continue to be taken; the current PNC user manual warns users that the PNC 'allocates a unique number to each transaction carried out by a particular user'[239] and that 'each transaction (enquiry or update) is recorded against a date/time reference by the computer'.[240]

Moreover, the cases illustrate is that training and guidance is provided to all officers about their responsibilities regarding the PNC.[241] This practice continues today; police staff with PNC access are able to use the 'PNC Training Bulletin Board' – an online provision containing 'PNC training related matters'.[242] Further guidance is provided in the PNC user manual, which states simply that 'users should be aware of the need to protect and handle personal data in accordance with the provisions of the Data Protection Act 1998'[243] and that '**the data is for policing purposes** only'[244] [emphasis in the original]. What is also

[236] J. Lewis, 'Hundreds of police officers caught illegally accessing records computer' *The Telegraph* (London, 20 August 2011)
[237] Above n.210
[238] Above n.211, [6]
[239] Home Office, 'The PNC User Manual' (v.15.02, December 2015) 26
[240] Ibid, 27
[241] Above n.211 [28]
[242] Above n.239, 28, para.11.1.
[243] Ibid, 28, para.12.3
[244] Ibid, 28, para.12.2

clear is that *some* officers are detected in their unlawful use of criminal records data and ultimately prosecuted. This indicates, at least, a degree of intent on the part of forces to investigate unlawful data processing and to prosecute where these are discovered.

These measures might explain the Commissioner's reticence to intervene. However, it is submitted that a more detailed examination reveals that the documentation assurances are undermined by serious flaws in some police force processes. The quality of the training being provided officers is certainly subject to question. As recently as 2005, for example, HMIC found that the Metropolitan Police had no written police regarding appropriate PNC use and that officers knowledge of their obligations regarding the data was so 'limited' that there existed a real risk of' inappropriate and unlawful use by staff'.[245] At West Mercia, there were some good training provisions in place but backlogs in rolling these out to all staff, so that 'officers who had requested PNC training and required it as a core part of their role are still waiting for it'.[246] At Northamptonshire, provision had been made for information security training to be provided by a bespoke computer package, but this was not being used and 'handouts' were being given to new staff during induction instead.[247]

Moreover, whilst police auditing of PNC checks has discovered hundreds of officers unlawfully and/or unauthorisedly processing data on the PNC, it is not known how many undiscovered instances have taken place. The police do not audit every PNC transaction. In fact, official police guidance on how many checks should be carried out recommends only that police check 'at least three transactions a day', although 'clearly a force which carries out a large number of PNC transactions would be required to check more than the minimum'.[248] It is not clear what, in the context of this guidance, constitutes a 'large number of checks', or whether such a force would be compliant with the guidance if it conducted perhaps four or five checks per day.

It is not certain that even this meagre baseline of transaction checks is being carried out; for example, HMIC inspectors found in 2005 that the Metropolitan Police were undertaking

[245] Her Majesty's Inspectorate of Constabulary, 'Metropolitan Police Service, Police National Computer Compliance Report' (14 – 18 February 2005) 16
[246] Her Majesty's Inspectorate of Constabulary, 'West Mercia Constabulary, Police National Computer Compliance Report' (12 – 16 December 2005) 12
[247] Her Majesty's Inspectorate of Constabulary, 'Northamptonshire Police, Police National Computer Compliance Report' (19 – 22 February 2007) 14
[248] ACPO, 'Data Protection, Manual of Guidance (Part II – Audit, 1 July 2007) 9

precisely no transaction monitoring.[249] A more persuasive instance of a data breach requiring urgent intervention by the Commissioner is difficult to envisage. Even where checks were being carried out, follow-up procedures by checking staff might not uncover unlawful use; in Suffolk Police, so many follow-up requests for evidence on why audited transactions had been made by officers came back with no supporting evidence that staff simply could not investigate them all,[250] while at Northamptonshire Police, the legality of the PNC check was 'automatically accepted with no further analysis' if the auditing officer thought the explanation provided 'looked legitimate'.[251]

It is, therefore, submitted that what is clear is that the number of instances of misuse uncovered must be only a small proportion of *actual* unauthorised and/or unlawful criminal record processing. The DPA 1998 requires that the police take *appropriate* (author's emphasis) technical and organisational measures to prevent unauthorised or illegal data processing. While the author accepts that some chief officers fulfilled their obligations[252] it is also clear that others did not, with some taking measures which were not appropriate in that they were insufficient to prevent avoidable instances of data breaches, while other chief officers appeared to be taking no measures at all so that their policies might reasonably be accused of facilitating breaches. It is for these reasons, and in these instances, that it is submitted that the Commissioner was in error in not intervening, and in the most egregious examples, in not issuing enforcement notices against the most recalcitrant chief officers.

6.6 Conclusions

This chapter has attempted to directly address the third research question and, it is submitted, in doing so it has demonstrated a number of *prima facie* breaches of data protection legislation by the police as regards their PHEONIX collection of criminal records. One of these alleged breaches, relating to the police failure to retain accurate and up-to-date records, seems to have been made out in the most irrefutable terms; the

[249] Above n.245, 15
[250] Her Majesty's Inspectorate of Constabulary, 'Suffolk Constabulary, Police National Computer Compliance Report' (6 – 10 June 2005) 9
[251] Above n.247, 13
[252] One example is Hampshire Police, who HMIC observed as implementing policies such that 'there is a culture within the force that the risk of misusing data is not worth taking because the chance of getting caught is high' – see Her Majesty's Inspectorate of Constabulary, 'Hampshire Police, Police National Computer Compliance Report' (10 – 13 October 2005) 12

problem was sufficiently widespread that even Parliament was sufficiently well-informed and concerned that they investigated the matter on more than one occasion.

The implementation of the DPA 1998 was intended to tighten data protection and give the ICO greater powers to investigate and sanction those responsible for it. However, for reasons which are not immediately apparent and for which no prescient explanation has ever been offered, the Commissioner failed to take any enforcement action against any police chief officer responsible as a data controller for the problems regarding the PHOENIX criminal record collection.

This is especially perturbing as regards the inaccuracies in the data, which have persisted for almost four decades, were widely publicised and which have caused subsequent hardship for thousands of affected individuals. This issue presented an ideal opportunity for the Commissioner to take the police to task; the *prima facie* evidence of a data protection breach was mountainous and independently verifiable, the impact on individuals was measurable, the attitude of chief officers unapologetic and there existed sufficient political and public criticism at the obvious police failings that the Commissioner's intervention would likely attract considerable support.

It is almost impossible to envisage any chief officers successfully resisting an enforcement notice issued circa 2000–2004 in respect of inaccurate data on PHOENIX. Such a notice might have also served to warn other chief officers that urgent remedial action was required.

It is submitted that the failure to issue any notice, on this or indeed any of the potential data breaches highlighted here, did precisely the opposite. It perpetuated the notion that the Commissioner was weak, or at least not sufficiently bold to take challenge police DPA 1998 breaches. It encouraged chief officers to do nothing more than pay lip service to data protection, safe in the knowledge that no immediate adverse consequences would flow from it. The practical reality, therefore, was that the fear of Lindop and his committee in 1978 had come to pass – in all but name, the police had obtained their exemption from data protection legislation.

7

The legality of the collection and retention of minor and inactive PHOENIX data

7.1 Introduction

It has never historically been the practice of the police in England and Wales to collect criminal record data for indefinite periods; Fosdick, for example, noted that the ordinary practice of the National CRO in 1913 was to delete the records of remand prisoners who were acquitted,[1] leaving them with a 'clean sheet'.[2] Even records which showed convictions might conceivably be expunged; during the inter-war years the practice of the National CRO was to 'constantly clear the records of dead men and those of still living men who are considered unlikely again to get into trouble'.[3]

Although the process undertaken by the police which determined who might be 'unlikely again to get into trouble' does not appear to have been documented, this supposedly systematic process of deleting records has been historically referred to as 'weeding'.[4] In later years, 'weeding' processes developed to expunge inactive records which show only old and minor convictions. This was considered desirable for several reasons. Some were simple practical considerations; weeding kept the physical records held at the CROs down to manageable levels, reduced storage costs and maintained a level of operational functionality. However, weeding has never been about merely restricting the space required to hold records. Extensive collections can give rise to policy concerns; MP Harry Cohen summarised that criminal record weeding was important because:

> The public need to be reassured that police records are not being kept for too long and that they are being used properly. There is also the widespread risk of such data being used for all sorts of different purposes that have more do to with big brother than effective policing.[5]

[1] R. Fosdick *European Police Systems* (The Century Company 1915) 328
[2] J.F. Moylan, *Scotland Yard and the Metropolitan Police* (G.P Putnam and Sons 1929) 195
[3] B. Thompson, *The Story of Scotland Yard* (The Literary Guild 1936) 220
[4] HC Deb 9 June 1964, vol.698, col.730
[5] HC Deb 20 February 1987, vol.110, col.1233

Moreover, the development of data protection legislation also appeared to provide further important backstops for the weeding of old records via the legal requirements that data held not be 'excessive' nor 'held for longer than necessary'.[6]

The purpose of this chapter is being to address the fourth, and arguably most difficult, research question. Here, the research intends to provide a critical evaluation of the retention of old, minor and 'inactive' criminal records by identifying, and evaluating, the key legislative, common law and policy developments which have resulted in the extensive, and near continuous, reformulation of weeding policies undertaken. This will provide the essential context required to address the fourth research question by the analysis which begins here but which follows more extensively in the following two chapters.

7.2 Weeding in the pre-data protection legislation period

By the middle of the 20th Century, it was evident to anyone seeking to establish the fact that old and minor criminality data was being weeded, but the precise procedures by which this was undertaken were far more difficult to ascertain. Indeed, as recently as 1964, a Home Office minister responded (somewhat reluctantly) to the threat of a writ being issued against a police force and the Home Office itself by confirming that:

> …old or trivial past convictions may be expunged from the record and [this] is carried out periodically...I believe that the House will bear with me if I refrain from disclosing in detail the circumstances in which that process is carried out.[7]

What emerged was that the police retained an absolute discretion on what, when and how data was 'weeded' from central records. It was only when James Rule observed staff in 1970 that a clear picture of the weeding 'policy' in place at the National CRO emerged. He saw that a juvenile record showing only one offence would be 'weeded' after ten years of no subsequent offending (referred to as a 'clear period'). For adults, records were weeded after a twenty-year clear period if the individual had only one conviction. Exceptionally, any record which showed a sexual offence was retained until the subject reached age seventy. Records with more than one offence were kept until age seventy,

[6] Initially Sch.1, part I, ss.4 – 6 of the Data Protection Act 1984, then Sch.1, part I, ss.3 – 5 of the Data Protection Act 1998.
[7] Above n.5

at which time they were weeded so long as the record showed a ten year clear period since the last offence.[8] Acquittals were supposedly deleted upon determination but there was significant variance between CROs; some deleted all acquittals, others exercised a discretion to retain files 'if police considered the matter exceptionally serious or sexual in nature'[9] while some simply 'routinely retain[ed] files on those acquitted'.[10]

Rule reported that National CRO staff claimed to have 'weeded' some 46,000 records between 1970–1971.[11] The problem, so far as Rule could see, was that there was no obvious means of identifying records which might be due for weeding, other than identifying the oldest records and checking to see if they met the weeding requirements. As a result, and in light of the obvious constraints of cost and manpower, Rule doubted that any systematic programme of record weeding existed, but rather that 'probably the staff exclude superannuated files as they encounter them, but little more'.[12] Parliament, again somewhat reluctantly, confirmed in 1972 that what Rule had identified was broadly accurate, save that single conviction records would only be deleted after the applicable clear period if the conviction resulted in a sentence of six months imprisonment or less.[13]

7.3 Weeding during the DPA 1984 period

When asked in Parliament immediately prior to the implementation of the DPA 1984, the Home Office confirmed that the (then) NIB implemented the same weeding policy as the CROs had operated in the 1970s.[14] In 1985, it was claimed by a Home Office minister that weeding was undertaken 'continuously, not only by NIB staff but also by individual forces and by the PNC itself'.[15] Quite how the PNC was able 'itself' to weed records is not clear – the PNC has never had an automatic deletion facility – and it is very likely that the minister spoke in error. In the same speech, the minister claimed that any PNC record against any individual who was subsequently acquitted and had no previous convictions recorded against them would be deleted.[16] What was not disclosed, until a further Parliamentary question required it, was that a microfiche record, falling outwith the scope of the DPA 1984, was retained by the NIB containing the original identifying number for

[8] J. Rule, *Private Lives and Public Surveillance* (Allen Lane, London 1973) 70
[9] Ibid, 67
[10] Ibid
[11] Above n.8
[12] Ibid, 71
[13] HC Deb 6 December 1972, vol.1972, col.1609
[14] HC Written Answers 18 May 1984, vol.60.
[15] HC Written Answers 28 June 1985, vol.81, col.519
[16] Ibid, col.521

any such deleted record. This was allegedly retained to 'prove that a record was deliberately destroyed and not lost or corrupted by the computer'.[17] Quite how data retained on a microfiche might reasonably be described as having been 'deliberately destroyed' is something the minister might have wished to clarify further.

Weeding of criminal records garnered wider media attention[18] in 1985 when the Home Secretary announced that new weeding procedures were being implemented 'to substantially reduce the number of criminal records held centrally without significantly impairing police effectiveness'.[19] These involved an expansion of the weeding policy to include the deletion of any record which showed a twenty year clear period, irrespective of the age of the offender and the number of previous offences, provided that the record contained no disposal of six months imprisonment or more, nor any homicide offences or sexual offences.[20]

This weeding procedure was justiciable in several ways. In an era of hard-copy recording, selective deletion would obviously save storage space and costs.[21] It also removes from searchable records those which are least likely to yield something of value. But it is submitted that this weeding criminal records was not, and was never, simply about saving space or money. Where a central data collection involves a significant proportion of the population, as was the case for the criminal record collection by the late 1980s, [22] weeding helps to assuage civil liberties concerns.

Moreover, this new weeding policy was an executive recognition that, although a small minority of individuals commit a disproportionately large number of crimes, very many individuals also come into contact with the criminal justice system a small number of times (or even just once) and then never do so again. The Government was merely reiterating that which the police had long predetermined; such records have little police operational value and there was, therefore, no pressing reason to retain them. This must explain why, at the time that computerisation opened up the potential for far greater storage than

[17] HC Written Answers 9 July 1985, vol.82
[18] 'UK news in brief: clean slate for petty offenders' *The Guardian* (Manchester, 15 March 1985)
[19] HC Written Answers 14 March 1986, vol.93.
[20] Ibid. These proposals were effectively codified into the first formal 'weeding' guidance produced by ACPO; see ACPO, 'Codes of Practice for Police Computer Systems' (1987)
[21] K. Younger, *Report on the committee on privacy* (Cmd 5012, 1972) para.436
[22] By 1987, one in eight of the adult population of England and Wales was the subject of a nominal listing on the PNC; see above n.5

previously conceivable, the initial response of the Government and the police was to delete, rather than retain, more criminal records.

The process was also a recognition by the police that they were conscious of, and apparently keen to adhere to (or at least be seen to be adhering to), the Fourth and Sixth Data Principles outlined in the DPA 1984. If the Government and the police both accepted that old, inactive criminal records have little operational value, then the lengthy retention of them might conceivably be challenged as 'excessive'. The police certainly thought so, and highlighted their weeding policy as evidence of compliance with the DPA 1984 in their 1987 Code of Practice, issued after direct consultation with the Registrar.[23] Indeed, the Registrar gave his cautious approval in a foreword latterly paraphrased as reading that the guidelines 'sounded all right, but that he would like to know what was happening in practice'.[24]

What was 'happening in practice' was that the problems identified by Rule persisted. MP Harry Cohen, one of the few MPs routinely questioning police use of the PNC, laid the charges to the Home Office in February 1987. He alleged that the Home Office recognised that weeding should take place but 'is not taking it seriously'.[25] This explained why, according to Cohen, since the introduction in 1985 of the more expansive weeding policing intended to 'significantly reduce' the number of records held, the collection had actually increased.[26] Indeed, the number of records weeded since 1985 was just 23,059; this equated to each member of staff allocated to the task weeding seven records per day.[27] This, Cohen claimed, pointed to a 'feeble weeding policy'.[28] The response of the Home Office was to retreat behind the lack of activity on the part of the Registrar; if there really was a problem, said the Minister, then 'individuals may make a complaint to the registrar, and the registrar has the power to look into it'.[29]

In 1987, ACPO agreed, subject to some very limited exceptions for homicide and sexual offences, that PNC records for individuals whose record showed a single offence would

[23] ACPO, 'Code of Practice for Police Computer Systems' (1987) para.4.2 and para.6.2. This guidance replaced the original APCO guidance document relating to the PNC issued in 1982.
[24] HC Deb 3 February 1992, vol.203, col.107
[25] Above n.5
[26] Ibid
[27] Ibid, col.1234
[28] Ibid
[29] Ibid, col.1238

be deleted after twenty years if there were no more offences recorded. Single caution records would be deleted after a three year clear period.[30] However, anecdotal evidence continued to surface supporting the contention that weeding was not being rigorously carried out; in 1992, the Home Office boasted that 60,000 records had been weeded in three months.[31] Closer examination reveals that this amounted to around 38 records per day weeded by each of the 18 staff supposedly engaged in the process. Meanwhile, *Liberty* complained that they had seen instances of cautions and convictions being referred to by police long after the period in which they should have been weeded.[32]

The Registrar was certainly conscious of the issue and was wary that records not be retained 'excessively'; in his evidence to the 1990 Home Affairs Committee he warned that the retention period for old, minor and inactive records should be 'carefully set'.[33] Despite this, and Cohen's allegations about the 'feeble' police weeding process, the Registrar did not take a more forceful approach to the issue and certainly no enforcement notices were issued against the NIB or individual chief constables.[34] It is not clear why the Registrar did not issue enforcement notices against the police where s/he was not satisfied that weeding was being undertaken in accordance with the approved procedure. It may be that the majority of the records to be weeded were not computerised, in which case the provisions of the DPA 1984 would not apply, but when in 1995 the PHOENIX application saw the computerisation of the majority of the records, the Registrar would have had the authority to intervene. It is submitted that the failure to do so, and the inherent flaws in the weeding processes, very likely meant that records were retained which should have been deleted and it is at least plausible that the police were emboldened by the lack of intervention so as to be demotivated to 'weed'.

[30] Above n.23, 13
[31] HC Deb February 1992, vol.203, col.111
[32] M. Colvin, 'The Criminal Record and Information System in England and Wales' (1992) 6 International Yearbook of Law Computers and Technology 139, 146
[33] Home Affairs Committee, *Criminal Records* (Cm 285, HC 1989 – 90, 3-I) 28
[34] The Information Commissioner, 'FOI Request. Information relating to enforcement notices issued to the National Identification Bureau' (Case Ref: IRQ0772425, *What Do They Know?* 1 August 2018). <https://www.whatdotheyknow.com/request/information_relating_to_enforcem> accessed 21 October 2018

7.4 Weeding during the DPA 1998 period

With PNC2 *in situ* and plans well advanced to add the NIB criminal record collection to it, in 1995 ACPO amended their weeding policy alongside their updated PNC Code of Practice[35] to incorporate 'general rules for criminal record weeding on computer systems'.[36] These maintained the general 'twenty year clear' rule for deletion but increased the exceptions to include certain specified violent offences, drug-related offences or those where the victim was a child or a vulnerable adult. The retention period for cautions was increased to five years.[37]

By late 1999, two important developments persuaded the police to again reconsider their weeding policy. The first was the passing of Part V of the Police Act 1997, which foreshadowed an imminent regime for employment and voluntary sector vetting on a hitherto unheralded scale. The second was the passing of the DPA 1998, which strengthened the enforcement powers of the Registrar/Commissioner to investigate instances of excessive data holdings[38]. Conscious of their apparent requirement to comply with the DPA 1998, in September 1999 an ACPO 'Crime Committee' approved a new 'Criminal Record Policy', specifically aimed at the retention of criminal records on PHOENIX, rather than merely incorporating this as part of the wider 'data protection' policy. This formed the substantive basis for the publication by ACPO in November 2000 of national guidance for the 'weeding' of PHOENIX criminal records data ('the 2000 Weeding Rules').[39]

The 2000 Weeding Rules made provisions under the general principle that 'the period of retention…will depend on the disposal types that it contains'.[40] The general rule was that an individual's nominal record would be deleted after a clear period of ten years.[41] This halved the time period which records would be held as compared to the previous regime. However, the exemptions to the new 'ten-year deletion' rule were much wider than previously; any record which showed a total disposal record of six months imprisonment or more (including suspended sentences),[42] three or more convictions (regardless of

[35] ACPO, 'Codes of Practice for Data Protection' (1995)
[36] Ibid, para.2.6.3
[37] Ibid, 20 – 21
[38] Per the Data Protection Act 1998, Schedule 1, Part I, ss.3 and 5
[39] ACPO, 'General Rules for the Criminal Record Weeding on Police Systems' (November 2000)
[40] Ibid, r.1
[41] Ibid, r.5
[42] Ibid, r.5.1

punishment on disposal),[43] an inability to plead due to insanity,[44] or any convictions for indecency, sexual, violent or one of the more serious drug offences[45] would not be weeded at all. Nor would any record which showed an offence involving the deliberate targeting of a child, elderly person or a disabled person[46] or any terrorism offence.[47] In all but one of these circumstances, the record was to be kept either until one year after the subject died[48] or until the subject of the record reached the age of one hundred years.[49] The exception was where the record contained three recordable but otherwise minor offences. These records were to be weeded after twenty years if no further offending was recorded.[50]

Any record which contained cautions but no convictions would be deleted after five years unless the record was accompanied by an 'offends against vulnerable person' marker.[51] The criteria for defining 'vulnerable person' was not expressed. Juvenile offenders who were given reprimands or warnings would have their record deleted once they reached (or passed) age eighteen and a five year clear period had passed.[52] The remainder of the 2000 Weeding Rules consisted of a list of offences which were to be 'retained for life'.[53] It was a lengthy list; fully eighteen pages detailing nearly 500 specified offences including those which are violent,[54] sexual,[55] involving serious damage to property[56] or serious drug offences.[57] No nominal records containing these would be deleted.

The 2000 Weeding Rules are important. They demonstrate that, at a time that the Government was pressing ahead with plans to enormously expand criminal record checks,[58] the police were implementing a national policy intending to continue the weeding of certain disposals out of the criminal record collection. Although in some ways more restrictive than previous policies, it nonetheless provided an implicit, continued concession from the police that not all records needed to be retained and that, over time, some lost

[43] Ibid, r.5.2
[44] Ibid, r.5.3
[45] Ibid, r.5.4
[46] Ibid, r.5.5
[47] Ibid, r.5.6
[48] Ibid, r.4
[49] Ibid, r.6
[50] Ibid
[51] Ibid, r.8
[52] Ibid, r.9
[53] Ibid, 6
[54] Ibid
[55] Ibid, 9
[56] Ibid, 12
[57] Ibid, 15
[58] See ch.8.5 of this research

their operational value sufficiently that their continued retention was not justified. So far as minor offending was concerned, the guidance effectively created a 'three-strike rule'; a tacit admission that the ACPO view was that a person is entitled to make two 'mistakes' until a third indicated a recidivistic nature justifying more extensive retention. It created a systematic procedure for 'weeding' based on three key denominators; the total number of disposals, the seriousness of the offence(s) and the time passed since the most recent disposal. Arguably the most important point, or at least the point which was to become more pertinent as the extended vetting regime began to permeate into society, is that the guidance related merely to the *retention* of criminal records, rather than the *disclosure* of them. Retention is far more justiciable than disclosure, and at the time that the Government was proposing for the widespread disclosure of criminal records, the police were implementing a policy which didn't see fit to even retain some of them.

The 2000 Weeding Rules were incorporated, almost in their entirety, into the ACPO Code of Practice for Data Protection 2002 ('the 2002 Code').[59] The 2002 Code, like the 1987 and 1995 Codes, was endorsed by a foreword from the Commissioner after discussions between ACPO and the Data Protection Registry/Information Commissioner's Office. On 17 September 2003, the Home Office issued formal guidance to the police relating to their few remaining vetting obligation which made specific reference to the importance of the 2000 Weeding Rules in helping 'to achieve compliance with the Data Protection Act 1998 [by ensuring] that information should not be retained for longer than is necessary'.[60] The Home Office specifically warned police officers that records due for weeding were no longer of 'operational value' and that, where a request for a police check brought such a record to attention, it must be deleted and the check should show a 'record of no convictions'.[61]

This could, and arguably should, have been the end of the matter. Formal weeding rules had been agreed between the three principal stakeholders and, so long as the police undertook their obligations under them, the ICO and the Home Office agreed that compliance with the two Data Principles would inevitably follow.

[59] At para.8.4
[60] Home Office, 'Circular 047/2003: Revised Arrangements for Police Checks', Home Office Circular (2003) para.15
[61] Ibid

7.5 *Bichard* and the first defeat of the Information Commissioner

This apparent unity was, however, a façade. This became apparent in the immediate aftermath of the *Soham* murders, which occurred almost simultaneous to the introduction of the 2002 Code. David Westwood, the Chief Constable of the force (Humberside Police) that had investigated four allegations of sexual offences against Ian Huntley in the 1990s, infuriated the Commissioner by publicly blaming him, and the DPA 1998, for their decision to delete the records from their local systems.[62] These claims were furiously refuted by the ICO, who sent out an Assistant Commissioner, David Smith, to retort that the decision by Humberside Police to delete records such as those relating to Huntley was 'astonishing'.[63] When the Home Office intervened by opining that they disagreed that the DPA 1998 hampered vetting, Westwood found himself defending his position on BBC's *Newsnight*. This culminated in him walking off set after telling Jeremy Paxman that his 'future was not in his own hands'.[64]

Tensions continued to simmer. In a (very) thinly veiled attack, the Commissioner told news media in January 2004 that his office intended to issue as much plainly drafted guidance as possible on the DPA 1998, so that 'people can never again use the excuse of hiding behind data protection'.[65] ACPO, for their part, proclaimed that the ICO was 'compounding confusion' on the issue by making representations to them to 'delete records' and further complaining that the Commissioner 'wants less offence details recorded on the PNC, not more'. This confrontational tone was more than simply an attempt to deflect attention from police errors uncovered by Bichard; ACPO had by this time formulated a new proposal for retaining criminal records which would allow them to retain all convictions on the PNC until the offender was dead or reached 100 years old.[66]

As part of his commission, Michael Bichard was tasked with investigating the 'record keeping' processes of the police as pertained to the *Soham* murders.[67] This inevitably meant a review of the weeding rules. Bichard found that individual forces were treating the weeding rules almost as if they were a type of malleable guidance, rather than fixed

[62] Q & A, 'Data Protection and the Police' *The Guardian* (Manchester, 18 December 2003)
[63] S. O'Neill and P. Stokes, 'Police chief faces axe for deleting Huntley records' *The Telegraph* (London, 19 December 2003)
[64] Ibid
[65] 'Data Protection guidance pledge' *The BBC* (London, 14 January 2004)
[66] 'Police attacked over Huntley data' *The BBC* (London, 24 February 2004)
[67] M. Bichard, 'The Bichard Inquiry Report' (HC 653, 22 June 2004) foreword

'rules' to be followed, and there was a wide variance in policy between constabularies.[68] Bichard also noted that the round of inspections into criminal records, conducted by HMIC to help rectify the chronic inaccuracies on PHOENIX, made no attempt to inspect or assess weeding procedures, it 'never previously surfacing as an issue'.[69] Giving evidence, Westwood admitted that neither the DPA 1998 nor the ICO were at fault for the deletion of Huntley's data. He also conceded that he had twice been warned not to blame the DPA 1998 for the deletion of the Huntley data; once by the Commissioner and again by the ACPO lead officer on sex offences.[70] The entire affair was most unseemly; Bichard commented that 'the unhelpful disagreement' was 'damaging to both [the ICO and ACPO] and is likely to have left the public, and serving police officers, less confident about how the legislation should be applied'.[71]

Bichard then considered the issue of retaining records and 'weeding'. He noted that criticism from ACPO at interventions by the Commissioner in respect of complaints made by the public was 'not fair', because that is the Commissioner's statutory role and because he had forewarned ACPO that he would do so in his foreword to the 2002 Code.[72] However, he chided the Commissioner for the tone of some of his interventions, saying 'it is one thing to ask searching and necessary questions. It is another to do so in an unnecessarily aggressive manner'.[73] Bichard recommended that a new Code of Practice be instituted, to ensure that any further 'confusion' as to the policy of record retention be alleviated. The policy needed to be 'clear, simple and designed to help police officers on the ground'[74] and should be drafted by the Home Office in conjunction with ACPO and the Commissioner.[75] At no stage did Bichard suggest, let more decree, that weeding be abandoned.

Nonetheless, Bichard opened his address as to the apparent conflict between the police position on criminality data and data protection by stating that 'data protection concerns are relevant but should not dominate the [new] code'.[76] He recognised that retention of

[68] Ibid 122, para.3.81
[69] Ibid 122, para.3.82
[70] 'Police warned twice over Huntley' *The BBC* (London, 25 March 2004)
[71] Above n.65, 128, para.4.5
[72] Ibid, para.4.6
[73] Ibid, para.4.7
[74] Ibid, 135, para.4.43
[75] Ibid, 136, para.4.44
[76] Ibid, 136, para.4.45

data, being less intrusive than using it (disclosure to third parties, for example) is 'easier to justify'.[77] Critically, Bichard noted that the Commissioner, in his evidence, had 'clearly and helpfully' indicated that 'the police are the first judge of their operational needs'[78] and, therefore:

> Police judgements about operational needs will not likely be interfered with by the Information Commissioner; his office cannot and should not substitute their judgement for that of experienced practitioners. His office will give considerable latitude to the police in their decision making. If a reasonable and rational basis exists for a decision, that should be the end of the story.[79]

What was evident was that *Soham* had significantly shifted the dynamic so far as criminal record retention was concerned. It is submitted that the Commissioner made two fundamental errors. The first was to misjudge the changed tenor of the retention debate. The Home Office and the police, both universally hostile to data protection for as long as it had been mooted, had found at last a way of justifying the circumvention of it. Concerns about excessively held data could be made to look misguided or even pernicious when portrayed as a barrier to the protection of children from dangerous sex offenders and murderers. The Commissioner seemed, it is submitted, not to have recognised the importance of this new justification for criminal record retention, and the difficulty he might have in attempting in future to circumvent it.

Secondly, it is submitted that the Commissioner erred in making comments in evidence which needlessly conceded ground to the very same chief police officers who had been flouting data protection legislation for two decades and against whom the blame for the vetting failures which led to *Soham* lay squarely and entirely. He allowed Bichard and the police to determine that data protection was, so far as police operational discretion is concerned, effectively a marginal concern. He accepted that the police are the principal judges of how to use their criminal record data, and those best placed to determine how long they might need to retain it. In doing so he conceded the very things to the police that the Lindop Committee had expressly refused to concede fully three decades earlier. The

[77] Ibid, para.4.45.5
[78] Ibid, 4.45.1
[79] Ibid, 4.45.2

gravity of these errors only became apparent in the various legal disputes which followed the publication of the *Bichard* report.

Perhaps understandably, the Commissioner was not especially pleased by Humberside Police's attempts to scapegoat him for their failures which contributed to *Soham*. The CRB opened in 2002 and, with Soham fresh in the public consciousness, was immediately inundated by millions of applications for criminal record checks.[80] The disclosure of very old and minor convictions on the new certificates issued by the CRB finally alerted members of the public to the fact that the police had retained criminality data on the PNC for a very long time. Some of those affected made formal complaints to the Commissioner, who duly instigated investigations into them and, when these bore little fruit, ultimately, and finally, resulted in the Commissioner issuing Enforcement Notices against a number of chief constables for alleged breaches of the DPA 1998 in respect of their PHOENIX collection of criminal records.

The Chief Constables of West Yorkshire, South Yorkshire and North Wales Police v The Information Commissioner[81] saw the police appeal to the Information Tribunal ('the IT') against three such Enforcement Notices. In the case of SY, a conviction for assault occasioning actual bodily harm from 1979 was recorded. SY was fifteen years old at the time of the conviction and was given a conditional discharge. No other convictions were recorded.[82] This came to light as part of a complaint made by SY against a neighbour, who was then a serving police officer. As part of the complaint process, the police force had checked SY's PHOENIX record.[83] By early 2003, the Commissioner had made various representations to the police data protection officer to have the conviction weeded to no avail and eventually an Enforcement Notice was served on 27 July 2004.[84]

A second complaint was made by WY, who had four offences recorded from April 1978 relating to theft of, and from, a motor vehicle and driving without insurance and whilst disqualified and another cluster of eight similar offences in February 1979. For two of these offences WY was sentenced to three months in a detention centre, to run

[80] C. Baldwin, 'The Demise of the Criminal Records Bureau' (17 February 2019) Journal of Criminal Law https://doi.org/10.1177/0022018319829290 3
[81] The Information Tribunal, 12 October 2005
[82] Ibid [10]
[83] Ibid [15]
[84] Ibid [22]

concurrently.[85] WY was 18 years old at the time of the second cluster of convictions. The designated police force data officer received correspondence from the Commissioner and duly refused to weed out the convictions.[86] An Enforcement Notice was issued on the same day as that regarding SY.[87]

A third complaint was raised by NW, who was convicted in 1967 (at age 18) of an offence under s.16 of the Larceny Act 1916. In August 1967 he was convicted of three further dishonesty offences and placed under a probationary order. A further larceny conviction was recorded in July 1968 and then, finally, three more offences were recorded in January 1969. These included taking a motor vehicle without consent and another larceny offence. NW was sentenced to (among other disposals) six months' custody during this period of offending and convictions.[88] A request to weed these convictions, the last of which was some 34 years subsequent, was refused and an Enforcement Notice issued on 5 October 2004.[89]

After almost two decades, the Commissioner had finally decided to take a stand against chief constables in respect of the PHOENIX collection. It is submitted that the Commissioner might have chosen his battle more carefully. In the cases of all three complainants, the police relied upon the 2000 Weeding Rules as justification for retaining the records. In all three instances, the police were *prima facie* so entitled; the single conviction against SY was expressly included in the list of specified violent offences which were to be retained for life[90] and both WY and NW were convicted for more than three recordable offences.[91] The offences in respect of WY and NW might have fallen to be weeded under the older policies of the 1970s and 1980s except that in both cases a cumulative total of six months custody was shown in the disposals, meaning that the records would be retained.

Quite why the Commissioner, after two decades of inertia regarding inaccurate, incomplete and unlawfully retained criminal records chose to issue Enforcement Notices

[85] Ibid [23]
[86] Ibid [29 – 30]
[87] Ibid [31]
[88] Ibid [32]
[89] Ibid [34]
[90] Above n.37, per rule 5.4 and Offence Code 1.8.12 The offence would have been weeded under any of the previous version of the weeding policies, though, had the Commissioner acted earlier his argument may well have carried more weight
[91] Per Ibid, rule 5.2

in three circumstances which fell squarely within the exceptions to the rules that he had endorsed only four years earlier is not clear. What is clear is that his assertion, in the case of SY, that the chief constable was in breach of the 2000 Weeding Rules by refusing to 'weed' out the conviction[92] was patently false and perhaps demonstrated a concerning lack of understanding of the very rules he had endorsed. That notwithstanding, it is also clear that the Commissioner himself (as he was then) took a personal interest in matters, attending a conference with the chief officers involved in the SY case in an attempt to persuade them that the record should be weeded.[93]

The IT found that there existed a difficult conflict between, so far as the police were concerned, the position that there 'could and can be no doubt that conviction history forms an integral part of the investigative operations of the police force'[94] and that vetting, as a form of crime prevention, constitutes a policing purpose,[95] as compared to the view of the Commissioner that, once a sufficiently significant 'clear period' of non-offending is evidenced, there exists 'no reasonable grounds for considering that the conviction data remained relevant for policing purposes'.[96] To support this, the Commissioner made reference to a Home Office study in 2001 which found that a significant proportion of the population had at least one conviction but that very few progressed to become recidivistic offenders.[97] So far as the police were concerned, however, a lack of further convictions did not necessarily mean that the individual was no longer offending but might mean simply that the person has 'learned how to avoid detection and conviction'.[98]

The view of the IT was that the Home Office study was not 'particular instructive'.[99] It also noted that two of the three cases involved multiple convictions, while the study focused on those with only a single conviction.[100] The IT was concerned that the 'empirical evidence on cessation [of offending after clear periods] is minimal, if not non-existent'[101] and that generally the actual tangible evidence provided by both parties was 'both sparse and over-generalised'.[102] Nonetheless, it accepted that criminal convictions, even 'minor'

[92] Above n.81 [14]
[93] Ibid [21]
[94] Ibid [100]
[95] Ibid [34]
[96] Ibid [76]
[97] Ibid [83]
[98] Ibid [107]
[99] Ibid [84]
[100] Ibid [86]
[101] Ibid [107]. It is submitted that such a finding is entirely incorrect; see chapter 8.4 of this research
[102] Ibid [201]

(and the IT emphasised the lack of clear definition as to what this constituted)[103] or aged convictions, had some operational value in policing activities, whether in offender profiling,[104] or in aiding investigating officers to 'trigger specific recollections' of use in individual cases[105] or even 'in general investigative work'.[106] The IT also recognised the use, and value, of convictions in the criminal justice process.[107]

Although concerned as to the over-generalisations offered regarding the quantitative value of the data in these purported uses, the IT reminded the Commissioner of his assurance to Bichard that he would not interfere lightly in the police judgement as to their operational needs.[108] Therefore, even though several of the purported uses were not formally recorded as purposes registered by chief constables with the ICO,[109] the IT was prepared to quash all three enforcement notices and permit the police to retain the data in accordance with the 2000 Weeding Rules.[110] However, in an amended order, chief officers were ordered that the retained data must be designated as not 'open to inspection other than by the data controller'.[111]

In short, the IT ordered that the data could be *retained* and utilised for police purposes, but it must not be *disclosed* (for example, as part of CRB vetting). This was, effectively, the fall-back position conceded by the Commissioner as an alternative, tenable position;[112] a 'step-down' process by which data would be retained by the police for their purposes but which, in certain specified circumstances, would be 'stepped down' on PHOENIX so that it could *only* [author's emphasis] be utilised for that purposes and not accessible by anyone else for anything else.[113] The IT were told that the police were in an advanced stage of producing such a 'step-down' model and they agreed that new guidance should be drafted to incorporate this, in co-operation with the Commissioner,[114] which should also

[103] Ibid [206]
[104] Ibid [208]
[105] Above n.101
[106] Above n.102
[107] Ibid
[108] Ibid [72]
[109] Ibid [220]
[110] Ibid [216]
[111] Ibid [218]
[112] Ibid [187]
[113] Ibid [50]
[114] Ibid [223]

dispense with the language of ‘weeding’ and make clear what is being retained and what is being deleted.[115]

So far as WY and NW were concerned, the decision of the tribunal was, to all practical intents, a victory. The police were prohibited from making the data available for vetting purposes, and so although the records would be retained, they would not have the immediate damaging impact on the lives of WY and NY that disclosure had created. For SY, the decision was a defeat. SY had not been subjected to a disclosure, and had wanted his data deleted. His data was to be retained. In all three case, the decision of the IT was a comprehensive defeat for the Commissioner. He had wanted the police to delete the data of all three subjects. Quite simply, the Commissioner had failed to persuade the IT that the retention of the data breached either the third or the fifth Data Principles. The police were told they could retain all three records in full.

It is submitted that the Commissioner failed because he made four fundamental errors which fatally undermined his case. The first is that he chose three cases where the individual records did not fall to be weeded in accordance with the 2000 Weeding Rules that his predecessor had expressly approved. To criticise the police after the event for applying these rules in the prescribed manner might reasonable be perceived to be churlish and gave the chief officers an extremely straightforward, and persuasive, defence to the Enforcement Notices and it is submitted that the Commissioner might have been better to have selected instances, or even waited (if necessary) to issue notices where complaints arrived where the 2000 Weeding Rules had been contravened.

It is further submitted that the Commissioner erred in failing to either identify or undertake the necessary research to demonstrate, at least on the balance of probabilities, that the retention of such data does not, as the police claim, have anything other than a notional benefit in operational policing purposes. The empirical weakness of the police case on this point was highlighted numerously by the IT but the Commissioner was unable to exploit this because his own counter-arguments were equally weak nor sufficiently evidence-based. That the IT was able to determine that there is a ‘non-existent’ empirical base for the desistence of most offenders from conviction, when there exists a significant

[115] Ibid [220 – 221]

repository of studies which show this as a near 'criminological constant',[116] illustrates sharply the Commissioner's failure to prepare accordingly.

The timing of the Commissioner's actions could also, it is further submitted, hardly have been worse. His Enforcement Notices against all three forces were issued in the immediate aftermath of the *Soham* trial and the subsequent *Bichard* report. At a time of heightened public fear of dangerous offenders, general sympathy (whether this be public, political, judicial or otherwise) for those who had criminal records could hardly be lower. In fact the rhetoric regarding 'protecting vulnerable people' from those who posed a 'known risk of offending' had hardened significantly and a 'vetting epidemic' had set in.[117] Quite simply, in an almost unprecedented atmosphere of heightened (indeed, at times, febrile) public concern regarding individuals who 'slipped through the net' because of a failure by police to properly record and use criminality data, the Commissioner chose to ask an IT to support his contention that the police must delete information of that very kind. A more mistimed tactical manoeuvre is difficult to envisage.

The Commissioner also found himself hoisted by his own petard so far as his comments to the *Bichard* Inquiry were concerned. He had promised that he would not 'lightly interfere' with the judgement of experienced police officers. He had also said that he would not substitute his own judgement for that of experienced practitioners. In this case, he could not show that the police were in breach of the rules, so instead he tried to argue that their view that the data had operational use was wrong. This allowed the police to paint a narrative of a Commissioner going back on the promise he gave to Bichard. It was, therefore, hardly a surprise that the IT could not support him. He was trying to do that which he said he wouldn't.

For all of these reasons, it is submitted that the Commissioner's decision to take a stand against chief officers in these three cases was misguided. In this author's view, he made a series of grave tactical missteps; as regards his decision to take action in the fact-specific circumstances of these particular cases, his decision to act at the time he did and also to represent on the basis that he did. Even accepting for the benefit of hindsight, it was not surprising that his challenge failed.

[116] This is examined at length at chapter 8.4.4 of this research.
[117] C. Baldwin, 'The Vetting Epidemic in England and Wales' (2017) 81 (6) Journal of Criminal Law 478, 485 – 492

7.6 The decisive second defeat of the Information Commissioner

In light of the *Bichard* recommendations, the legislative amendments which permitted the permanent retention of other sensitive criminality data, such as DNA and fingerprints, even where the suspect is acquitted[118] and doubtless emboldened by their victory over the Commissioner at the IT, ACPO pressed ahead with the creation of their replacement for the 2000 Weeding Rules. Published in 2006 ('the 2006 Guidelines'),[119] these expressly superseded all previous rules and guidelines[120] and deviated quite substantially from that which they had postulated as forthcoming during the *South Yorkshire* case. The 2006 Guidelines entirely abandoned the process of weeding any records and were instead 'based on restricting access to PNC data, rather than the deletion of that data'.[121] In short, the new guidelines provided that where a nominal record was created on PHOENIX, regardless of whether it related to a conviction, caution, PNfD, acquittal or even an arrest, then the record was to be retained on PHOENIX until the subject reached the age of 100 years.[122] This was justified as 'providing the police service with continuous access to data that will allow it to discharge its responsibilities'.[123]

The general disclosure principle underpinning the 2006 Guidelines was that access would be controlled via a 'step-down' process. This meant that retained data would, after specified time periods, be marked 'for police eyes only' and so not disclosed to any non-police body unless the data fell to be released under the s.115 Police Act 1997 provisions regarding 'enhanced' CRB certificates.[124] The 'step-down process' itself was extremely complex. The most serious offences were described as 'Category A' offences and where an adult[125] or a young person[126] was convicted such an offence and subsequently received any custodial sentence then the entire criminal record of that individual would never be stepped-down. The list of Category A offences consisted of fully 37 A4 pages[127] and included the more grievous violent, sexual and drug-related offences as well as somewhat

[118] Per s.82 of the Criminal Justice and Police Act 2001, amending s.64 of the Police and Criminal Evidence Act 1984. These provisions were successfully challenged and this is evaluated at length in chapter 9.4 of this research
[119] ACPO, 'Retention Guidelines for Nominal Records on the Police National Computer. Incorporating the Step-Down Model' (March 2006)
[120] Ibid, para.1.1
[121] Ibid, para.1.3
[122] Ibid, para.3.1
[123] Ibid, para.3.2
[124] Ibid. These are discussed at para.8.5 of this research.
[125] Ibid, para.4.1 and para.4.7
[126] Ibid, para.4.4 and para.4.10
[127] Ibid, 18–55

more unusual crimes, such as 'violating the King's wife' and 'slaying the Lord High Chancellor'.[128] Differing step-down periods applied for Category B and Category C offences depending on the age of the offender and the disposal on conviction; an adult committing a Category C offence which resulted in a six month sentence (or longer) would be stepped down only after 30 years. These included such disparate offences as neglecting to maintain a wife,[129] misconduct on a railway,[130] knowingly failing to cause regular attendance at school of a pupil[131] and selling cigarette lighter fluid to persons aged under 18.[132]

Far more stringent though this new regime was, there remained a recognition that those with minor disposals should be treated with more leniency than more serious offenders, with 'minor' being seemingly determined in accordance with the disposal made in individual cases; indeed, even Category A offences committed by adults would be stepped down after twenty years if no custodial sentence was handed down.[133] The stepping down period for similar offences committed by juveniles was fifteen years.[134] Non-custodial disposals in Category C offences would be stepped down after twelve years for adults[135] and ten for juveniles.[136] Cautions were to be stepped down in either ten years (Category A offences)[137] or five years (Category B and C)[138]. The same periods applied to reprimands and final warnings.[139]

The 2006 Guidance marked a significant change in tack on the part of the police. What was apparent was that the almost lackadaisical attitude evident in the maintenance and general retention of criminal records evident prior to *Soham* had metamorphosized into a hitherto unprecedented, hard-line approach which aimed to solve the problem of inconsistent record deletion by deleting nothing at all. The decision to start from the position of holding records until the subject is aged 100 years appeared entirely arbitrary and marked a significant departure from all past guidance and procedures and had not

[128] Ibid, 40
[129] Ibid, 100
[130] Ibid
[131] Ibid, 101
[132] Ibid
[133] Ibid, para.4.13
[134] Ibid, para.4.16
[135] Ibid, para.4.15
[136] Ibid, para.4.18
[137] Ibid, para.4.19
[138] Ibid, paras.4.20–4.21
[139] Ibid, paras.4.22–4.24

been expressly supported by anything said or done in either in *Bichard* nor the *South Yorkshire* case. With the benefit of hindsight, this policy should be viewed, it is submitted, as flagrant attempt by an emboldened ACPO to revert to the position they held prior to the implementation of data protection legislation; making decisions entirely of their own accord and unfettered by any imposition from any external body.

Unsurprisingly, the Commissioner was wholly unimpressed by the 2006 Guidelines. He had been consulted by ACPO during the construction of them but his position was so contrary to that of ACPO that he refused, for the first time, to endorse the published guidance.[140] In the meantime, more complaints were being made by members of the public who were distressed to find that aged criminal disposals were still being kept on the PNC. In response, the Commissioner elected again to issue Enforcement Notices against data controlling chief constables. The Commissioner seemed to have learned from his prior mistakes; he at least selected five more 'meritorious' possible candidates for record deletion. The first, HP, was aged sixteen when he was convicted, alongside another juvenile, in 1984 of a shop-theft and fined £15. This conviction was retained on the PNC in 2006, when it was disclosed for employment vetting purposes.[141] It is perhaps worth noting that this conviction should not have been held on the PNC by that time. In fact, it should have been deleted in 2000, which was the expiration date of the ten-year clear period established by para.5 of the 2000 Weeding Rules for such single, minor offences.

The second individual, SP, was given a reprimand at age thirteen for punching and kicking a fifteen-year old girl in 2001. This was disclosed to a potential employer in 2006.[142] This reprimand, being the single police contact on the record, would also have been deleted under the old weeding rules and indeed SP was told it would be at the time it was issued,[143] but it was evidently retained because the rules in force at the time of issue were not the rules in force at the time SP reached eighteen years of age (at which point the reprimand would have been expunged under the old rules). A third individual, NP, was convicted of two obtaining by deception offences in 1981.[144] No other offences had been recorded so, once again, this record fell to be expunged in 2000 when the 2000 Weeding Rules came

[140] The Chief Constable of Humberside (and four others) v The Information Commissioner, Information Tribunal Appeal Numbers EA/2007/0096, 98, 99, 108, 127, 21 July 2008 at [4]
[141] Ibid [66]
[142] Ibid [69]
[143] Ibid [70]
[144] Ibid [72]

into force. The revelation of the offences on an employment vetting check confirmed that the record was still held.[145]

The fourth individual, WMP, was convicted of two attempted theft offences and an offence of criminal damage when, as a fifteen-year old in 1978, he inserted 'mental blanks' instead of coins into an arcade machine.[146] No other convictions were held against WMP but this record did not stand to be retained under the 2000 Weeding Rules as it contained three separate offences. However, it ought to have been due for deletion in 1998, as the record had been inactive for twenty years at that point and therefore a candidate for weeding under the 1995 'twenty-year rule'. The final individual, GMP, had been convicted at age 19 of theft in 1983, and asked for two other offences to be taken into account. No other convictions were recorded but, under the 'three strikes' rule, the record stood to be retained under the 2000 Weeding Rules. That the record still existed only became evident when GMP made a DPA 1998 subject-access request to support her plan to emigrate to St. Lucia.[147]

The IT convened to hear the appeals against the Enforcement Notices made by all five chief constable Data Controllers recognised that four of the records should have been weeded long ago. In response, the police admitted, for the first time, that 'weeding did not take place proactively' and in actuality this only occurred after a request for removal was made by an individual. Even the 'stepping down' of data was not done proactively and only took place after a request to do so.[148] This, it is submitted, illustrated that ACPO's policy as regard the retention and deletion of criminality data was nothing less than fraudulent: written policies, drafted in consultation with, and in an attempt to assuage concerns raised by, the Information Commissioner to ensure compliance with the DPA 1984 and the DPA 1998 were, in fact, little more than a paper exercise. The reality was that the concerns raised by Harry Cohen as early as the 1980s were entirely justified and, if anything, had underestimated the scale of the problem. The police were not even pursuing a 'feeble' weeding policy. They were, in fact, pursuing no weeding policy of any material kind whatsoever and were instead simply retaining records until or unless they were told not to.

[145] Ibid [73]
[146] Ibid [74]
[147] Ibid [76]
[148] Ibid [78]

The reality was that the 2000 Weeding Rules, like all of those before them, were a sham; simply documents to which ACPO could point to 'demonstrate' data protection compliance but which had no practical impact on the retention of criminal records or compliance with the DPA 1984 or the DPA 1998 at all. In actuality, the police had never been in compliance with the third and fifth Data Principles. It is little wonder that the Commissioner felt compelled to issue Enforcement Notices. He had approved repeated retention policy documents under false pretences. For decades, he and his predecessors had been entirely misled.

The IT was asked to consider whether the retention of all criminal records under the 2006 Guidelines was excessive and/or for longer than necessary. To answer this question, regard was given to the purposes of holding the data. The chief officers argued that this must be read in accordance with all of the possible uses of the data[149] (particularly the use of records for criminal vetting purposes).[150] The Commissioner took an entirely different view, and argued that compliance with the DPA 1998 should be read in accordance only with what he called 'core' police purposes; namely the prevention and detection of crime, the investigation and apprehension of offenders and the maintenance of law and order.[151]

On this point, the IT found in favour of the Commission. It held that 'in data protection terms, this processing requires holding criminal intelligence on the PNC for so long as it is necessary for the police's core purposes'.[152] Where this impacts on the ability of the police to provide data to the CPS, courts or other external agencies, it is immaterial because 'Chief Constables are not required under their statutory obligations to hold data they no longer require for core purposes. They are only required to provide data they do hold at the time of the request'.[153]

In short, 'Chief Constables cannot be expected to incorporate other bodies' purposes as part of their own, even if there is some common objective'.[154] This was substantiated by reference to the Police Act 1997, which authorises criminal record use for employment vetting purposes, and which states[155] that 'any person who holds records of convictions

[149] Ibid [91] See chapter 4 for a full exposition of these.
[150] Ibid [95]
[151] Ibid [90]
[152] Ibid [96]
[153] Ibid
[154] Ibid [97]
[155] At Part V, s.119(1)

or cautions for the use of police forces generally shall make them available to the Secretary of State'. The IT found that 'if the information is no longer held [because it has been deleted because it no longer serves use for police purposes] then there is no obligation [to provide it for vetting purposes].[156] The IT concluded on this point by noting that the PNC 'had evolved over the years and it is now regarded as the main source of criminal intelligence for a variety of organisations'.[157] However, it is bound by no statutory framework and those involved predominantly in its administration, such as ACPO and NPIA are not registered as data controllers. The Tribunal's view was that if the intention was for the PNC to be used in this manner, it was for Parliament to legislate accordingly as this would 'provide the opportunity for Parliamentary debate on how best to provide an appropriate and proper legislative framework so that there is a clear understanding of data ownership and obligations with proper safeguards'.[158]

The IT then moved to consider the other police 'justifications' for retaining old and minor criminal data beyond the 'core' police purposes. The Chief Constables argued that they were also obligated to retain all conviction data for the 'prosecution of offenders'; in short, the PNC record was required to assist the CPS in prosecutions and for 'bad character' purposes.[159] The Commissioner, with whom the IT agreed,[160] argued that the police had always deleted old and minor criminal records so that they must not have previously felt obligated to hold all records, nor do the police have any legal obligation to do so and, in any event, that retaining criminal records which no longer serve any useful function for 'core' policing purposes can only be justified if a specific legislative provisions mandates it.[161]

Similarly, the ITT accepted the Commissioner's view that the proper interpretation of the police role in MAPPA and other work was 'that the police are cooperating with other agencies in order to achieve the objective of preventing crime', not that this work had 'extended' the purposes for which police hold criminality data.[162] The Tribunal was also not convinced that retaining old and minor conviction assisted in the location of missing

[156] Above n.140 [98]
[157] Ibid [99]
[158] Ibid
[159] Ibid [102]
[160] Ibid [104]
[161] Ibid [103]
[162] Ibid [106]

persons, despite police claims to the contrary.[163] That is hardly surprising; it is difficult to envisage how a twenty year old conviction for theft might assist in the location of missing persons in any manner whatsoever. This left for consideration the use of criminal records for employment purposes. The IT accepted that the disclosure of criminal records might play a part in the prevention of crimes against vulnerable children and adults, but the Commissioner argued that where records no longer have any use for that purpose so long as the police are considered, it must follow that they also serve no concurrent purpose to employers. The IT agreed, and provided that 'it is not the function of the police to run an information service for prospective employers helping them to assess, in general terms, whether they wish to employ particular individuals'.[164]

The remaining question, then, was whether the retention of old and minor conviction data, such as that held against the five named individuals, did, in fact, continue to serve some useful purpose so far as the 'core' policing purposes were concerned. On this issue the Chief Constables once more relied, almost entirely, on the submissions made to Bichard by the Commissioner that they, not anyone else (and certainly not the Commissioner) are the first judges of their operational needs.[165] This position was bulwarked by the Home Office, which had by now completely reversed their position from that in 2003 which provided that the police needed to continue to delete data, and were instead postulating that the provisions of the Police Act 1997 effectively meant that Parliament had considered the issue of whether holding all convictions was DPA 1998 compliant and answered in the affirmative.[166]

Once again, however, on this point the Commissioner had clearly learned from his mistakes in the *South Yorkshire* case. This time he argued that, although he stood by his comments to Bichard, these had to be read, as did the third and fifth DPA 1998 principles, in accordance with Article 8 of the European Convention of Human Rights which enshrined a right to privacy[167] which might only be displaced when 'necessary' and 'proportionate'.[168] The chief officers adduced evidence which suggested that past convictions had helped

[163] Ibid [112]
[164] Ibid [109]
[165] Ibid [116]
[166] Ibid [117]. It is difficult to see the rationale in the Home Office position – quite how Parliament, in passing the Police Act in 1997, were implicitly conferring compliance with data protection legislation not yet entered into the legislative stream, is not readily apparent.
[167] At Article 8.1 of the European Convention on Human Rights 1953
[168] Above n.140 [121] and Article 8.2 of the ECHR

solve longstanding investigations, but the Tribunal found that 'few, if any, of these examples seemed to relate to the sorts of offences committed…in this case'.[169]

By contrast, the Commissioner adduced evidence from an Assistant Information Commissioner, who had thirty years of experience as a police officer, which claimed that none of the retained information in the instant cases had any continuing value for policing purposes.[170] Indeed, it was accepted in evidence by the chief officer in the GMP case that the initial response to the Enforcement Notice issued in that matter had been a recommendation to delete the data as required; it was only two days later that this position was reversed at the insistence of ACPO[171] who were keen to ensure that the chief officer presented a 'united front' in the defence of the general position provided by their 2006 Guidelines.[172]

Moreover, the Commissioner, doubtless chastened by his failure to adduce persuasive, empirical evidence in support of his claim that the holding of old and minor criminal records was excessive to the IT in the *South Yorkshire* case, this time commissioned two academics to make the point for him. He asked the same two academics who the Home Office had commissioned to review patterns of offending in 2001, Brian Francis and Keith Soothill, to undertake a detailed statistical analysis of the old police adage that 'old records attach new crimes to old criminals'.[173] Francis and Soothill's evidence was sufficiently robust that the expert commissioned by the chief officers to counter it was unable to much dispute it, instead electing to try to 'add' to it.[174] It is perhaps unsurprising, therefore, that the Tribunal determined the evidence as providing 'an objective basis upon which [they] can consider the Enforcement Notices in this case'.[175]

This evidence suggested that, taking into account the relatively minor nature of the convictions recorded, the age of the convictions, the age of the individuals at the time of the convictions and the disposal of the court in each case, that HP had no more than a 1.6% of reoffending in the next five years, as opposed to a general rate among non-

[169] Above n.140 [123]
[170] Ibid [124]
[171] Ibid [77]
[172] Ibid [146]
[173] Ibid [125] The analysis formed the substantive basis of a subsequent academic journal piece; see B. Francis and K. Soothill, 'When do ex-offenders become like non-offenders?' (September 2009) 48 (4) The Howard Journal of Crime and Justice 373
[174] Above n.140 [126]
[175] Ibid [127]

offenders of 0.7%.[176] Identical analysis showed that the likelihood of reoffending for WMP to be exactly the same as HP,[177] while that of NP was halved to 0.8%.[178] The reoffending probability of GMP was held to be the same as NP.[179] A similar analysis of SP could not be carried out because of the relative recency of her reprimand but the Tribunal heard that, in one further year, based on her age, her being female (whose offending rates generally are much lower than men) and the minor nature of the offence, there would be 'little difference' in terms of her propensity to reoffend as compared to a non-offender.[180]

The question for the IT, then, was what to do about the Enforcement Notices. The Home Office, intervening alongside the chief officers, argued that the 'step down' model was incompatible with the requirement to disclose all records held on the PNC in the specified circumstances laid down in Part V of the Police Act 1997.[181] That, it is submitted, was a logical and irreconcilable position, and it was therefore left for the IT to accept that the police were indeed obliged to release all conviction data held. In practical terms, this meant that the 'step-down' procedure could not stand unless the police were able and willing to 'step down' the relevant material to some resource outwith PHOENIX. The obligation on chief officers is to release all data held in 'central records' – if the data was held elsewhere, the obligation might not apply.[182]

In any event, however, the Enforcement Notices required the data be 'stepped out' (i.e. deleted completely), rather than 'stepped down'. The Tribunal, for all of the reasons offered by the Commissioner, ultimately upheld each notice.[183] It summarised the reasons for doing so as being that:

> Chief Constables are required to process personal data, including conviction data, in accordance with their statutory obligations under the DPA. If such compliance requires the erasure of conviction data…then that information will no longer be held on the PNC.[184]

[176] Ibid [134]
[177] Ibid [143]
[178] Ibid [140]
[179] Ibid [145]
[180] Ibid [138]
[181] Ibid [182]
[182] Ibid [185]
[183] Ibid [207]
[184] Ibid [205]

The judgment of the IT was an extremely detailed and measured one. It was also commendable in numerous respects. The IT's reading of the applicable legislation was extremely detailed and persuasive. It is submitted that their reading of s.27(4) PACE 1984 was of particular importance. That provision is permissive, not mandatory.[185] It says that a central record of convictions '*may* by regulation' be kept, not that it *must* [author's emphasis]. Parliament, in drafting s.27(4), simply must have known that the police have never attempted to make a complete collection of all criminal records, to be held to all intents and purposes for the life of each individual concerned. Certainly, that was not the policy of the NIB when PACE 1984 was drafted.

Similar considerations must, it is submitted, be brought to bear as regards the Police Act 1997. Parliament must have known there existed a policy of weeding at the time that legislation was passed and this, it is submitted, is required in the language of the legislation, which provides that the information used for disclosure purposes is simply that 'held in central records'. There is no legislative requirement to record all conviction and other disposal data indefinitely. Furthermore, the continued implementation of Regulations relating to recordable offences illustrate that Parliament do clearly know, and must continue to intend, that the collection of criminal records remain incomplete. If it intended otherwise, it is submitted that it must surely legislate as such.

Additionally, the decision of the IT not to simply defer to the police on the supposed operational value of the PHOENIX collection was perhaps the first time that anyone had done so in a public forum. For well over a century, Parliament had simply accepted, apparently without any critical thought, the police assertion that criminal records helped them 'do their job', therefore the records should be retained. *Bichard* had done almost precisely the same when assessing the matter after *Soham*, as did the tribunal in the *South Yorkshire* case, which accepted almost entirely the same blithe assertions the police had made on this point to Bichard.

Here, the IT took a different approach. It heard detailed evidence from experienced police officers and the tribunal examined them on precisely how these records actually assist at operational level. In response, the police officers were unable to provide any specific answers or persuasive explanations. They continued to rely upon anecdotal and irrelevant

[185] Ibid [19]

examples which bore little or no resemblance to the issues at hand. The reality – that very old and minor criminal conviction data has little, or indeed no, operational benefit in the prevention of crime and the detection of offenders – which had been suspected by some for decades but never fully brought into a public forum, was laid bare in the starkest terms. When pressed, for the first time, to properly account for their assertions, the police were found wanting.

The justification for that approach lay not just in the weakness of the police' case but also in the ITs willingness to admit, and to accept, expert evidence on just how much operational value old and minor convictions are likely to have for policing purposes. This marked the first, and to date the only, time any tribunal or court in England and Wales has heard any empirical, quantitative evidence pertaining to the 'usefulness' of old and minor criminal data as a means of preventing further offences or investigating existing ones. What it found was that the data had either very little or no value whatsoever for those purposes. The evidence of Soothill and Francis was so persuasive that the police expert, appointed no doubt to discredit it, found himself largely agreeing with it. It is perhaps unsurprising, then, that the tribunal found the evidence as appealing as it did.

The Commissioner deserved some credit. After making several fundamental errors in the preparation of his first set of challenges in the *South Yorkshire* case, here he rectified these and brought a far more persuasive case. He saw that the *South Yorkshire* IT had felt unable to displace the statement the Commissioner had made to Bichard in the absence of evidence to the contrary and so sought expert evidence to try do so. He adduced evidence from ex-police officers in an attempt to counter the anticipated police assertions as to the value of the data. His selection of individuals' records to contest was far better, and indeed, this also demonstrated the duplicitous police position as to the actual weeding of records. The police position lacked credibility because the Commissioner was able to show that the police had been lying, consistently, for decades.

The Commissioner was rewarded with a comprehensive victory. He had sought to have the 2006 Guidance declared as unlawful and he entirely succeeded. He elected made his fight public from the outset; while the *South Yorkshire* case passed almost without anyone much noticing, the Commissioner in the latter case announced publicly his issuing of

Enforcement Notices.[186] In doing so he risked making a second failure to take the police to task a very high-profile one. Instead, his success attracted widespread press attention.[187] After years of apparent deference to the police as regards possible data breaches, the Commissioner had finally challenged the police and won. The implication of the decision was clear – records, potentially millions of them, would have to be deleted.

An ICO Assistant Commissioner told the media that the IT had passed a 'landmark' judgment which would prevent further 'harm and distress caused by the retention of this data'.[188] ACPO, meanwhile, declared themselves 'disappointed' with the decision and reported that chief officers would discuss what to do next.[189] What they ultimately decided to do was appeal to the Court of Appeal. It was the first time any question of data protection had reached the appellate courts and the decision in what became known as the *Five Constables* case[190] must have dealt a devastating blow to the Commissioner. The lead judgment was delivered by Waller LJ, whose pronouncements must be sharply contrasted with the detailed and precise scrutiny offered by the IT at first instance. He opened his decision in auspicious fashion; immediately demonstrating his lack of understanding of record weeding by claiming that 'his reading' of the background 'leads me think that ACPO (without consultation with, for example, the CPS and the courts) were persuaded that data protection principles should lead them to have what was termed a 'weeding policy''.[191]

As this research has shown, 'his reading' was demonstrably wrong: a policy of weeding records has existed long before data protection, or indeed ACPO, were formed. His understanding of the PNC and PHOENIX seemed little better, with it being claimed that s.27(4) provides 'the statutory authority' for the PNC. That statement is also demonstrably false – the provision makes no reference to the PNC and, indeed, the PNC went live some eleven years prior to the provision's enactment: presumably then the PNC had no 'statutory authority' during that inception period.

[186] 'Police told to delete old criminal records' *The Guardian* (Manchester, 1 November 2007)
[187] See, for example, 'Criminal records must be erased' *The BBC* (London, 22 July 2008) and J. Oates, 'Police told: delete old criminal records' *The Register* (22 July 2008)
[188] 'Criminal records must be erased' *The BBC* (London, 22 July 2008)
[189] J. Oates, 'Police told: delete old criminal records' *The Register* (22 July 2008)
[190] *Chief Constable of Humberside Police and oths v The Information Commissioner* [2009] EWCA Civ 1079
[191] Ibid [2] (Waller LJ)

Undeterred, after summarising the arguments on both sides (which remained largely unchanged), the applicable facts and the relevant legislation, the Court then considered the detailed findings of the IT as regards the permissive nature of the collection. It did so in precisely one paragraph, noting that '[the Tribunal found that] the PNC would not be complete record of all conviction. That may be true, but I am doubtful as to its relevance'.[192] That, it is submitted, was unfortunate, because the IT had, in the most explicit and persuasive terms, detailed precisely why the permissive nature of the PHOENIX collection was very relevant indeed. In fact, it is submitted that the proper reading down of the legislation requires a detailed consideration of precisely that point.

This oversight was especially important, because the Court then moved to consider the Commissioner's view, accepted by the IT, that criminal record data could only be held for 'core' police purposes. It rejected these arguments and said that, in having accepted this base proposition regarding 'core purposes', the IT had 'got itself off on the wrong foot'.[193] Indeed, such an approach:

> …misconstrues the Data Protection Act 1998…The data controller must specify the purpose for which data is retained [but] there is no statutory constraint on any individual or company as to the purposes for which he or it is entitled to retain data. I would accept that the purposes must be lawful…but, that apart, a data controller can process data for any purpose'.[194]

The police had registered their PHOENIX repository under a variety of different 'purposes'. Waller LJ accepted the view that the police registered purpose of 'rendering assistance to the public in according with force policies'[195] 'clearly covers the role' that PHOENIX has in providing complete lists of convictions to the CPS, the courts and the CRB (further evidenced by the listing of recipients to include 'employers', 'the courts' and 'law enforcement agencies).[196] Once more it is not difficult to find fault with such an analysis; quite what 'force policies' encompass such a role was never explained and this author suggests that no such policies exist, while it is also not clear how providing a list of convictions to the CPS or to the Courts provides assistance to 'the public'. This very point

[192] Ibid [23]
[193] Ibid [36]
[194] Ibid [31]
[195] Ibid [34]
[196] Ibid [35]

was, in fact, conceded by Carnwath LJ, who recognised that these might best be described as 'public agencies', rather than 'the public in general'.[197]

Nonetheless, the view of the court was that the police had registered these purposes and these were as valid a reason to retain criminal records as 'core policing purposes'.[198] With this in mind, and so long as these reasons were those which had been registered at with the ICO (which they were),[199] then 'if one then poses the question whether the Data being retained is excessive or being retained for longer than necessary for the above purposes there is, it seems to me, only one answer, since for all the above a complete record of convictions, spent and otherwise, is required. That seems to me to be a complete answer to the appeal'.[200]

Even if the this analysis was incorrect, and that the data retention could only be justified as regards 'core' policing purposes, then nonetheless the view was that the IT 'went wrong in this case'.[201] Waller LJ declared that the view the IT had taken regarding the statistical evidence offered by Soothill and Francis being 'helpful' was simply 'wrong'.[202] His subsequent review of the 'evidence' concerning 'core purpose' of the data was very different to that of the IT. Instead, he reverted to the position offered by the IT in 2005 in the *South Yorkshire* case; namely that the Commissioner had told *Bichard* that he would not substitute his judgment for that of the police. That, he said, was 'the correct approach'.[203] He accepted the evidence, rejected as too vague by the Tribunal, provided by officers that old and minor data can be of use in profiling offenders, identifying possibly dangerous individuals or providing evidence in current or future cases.[204] Where the IT had criticised this evidence as vague and unpersuasive, by contrast the Lord Justice found

[197] Ibid [85], although he then accepted that the problem could easily be rectified by the police amending their registration details, which would offer little aid to the Commissioner or the data subjects (ibid [91]). This position demonstrates once more the general appreciation of the applicability of data principles or the legislation purporting to them; as Treacy and Terelgas noted; 'this approach overlooks the fact that an updated notice would not apply retrospectively to the data already held' – see B. Treacy and A. Terelgas, 'Under the spotlight: police retention of conviction data' (1 February 2010) 10 (3) Privacy and Data Protection Journal 12
[198] Ibid [35]
[199] Ibid [34–35]
[200] Ibid [36]. It is submitted that this approach is entirely incorrect because it is based upon a wholly inaccurate base proposition. A full exposition of by this is so is provided in the next chapter of this research, and also at chapter 4
[201] Ibid [39]
[202] Ibid [42]
[203] Ibid [43]
[204] Ibid

that ‘the evidence is very much that the information might be of value in certain circumstances and of value when taken together with other information.[205]

Even if the IT had been correct in its approach so that only the ‘core purpose’ was relevant, then their reliance on statistics showing the risk of future offending in such cases to be very slightly greater than for non-offenders ‘was not something I [the judge] would pray in aid’.[206] The Lord Justice concluded that:

> If the police say rationally and reasonably that convictions, however old or minor, have a value in the work they do that should, in effect, be the end of the matter. It is simply the honest and rationally held belief that convictions, however old and however minor, can be of value in the fight against crime and thus the retention of that information should not be denied to the police.[207]

Therefore, unless the view of the police was perverse or unreasonably held (which the Court did not believe it to be), then the data should all be retained.[208] Any attempt by the Commissioner to insist otherwise was, said the court, an attempt to misconstrue the purpose of the DPA 1998 in an attempt to ‘overrule the will of Parliament by a side wind’.[209] Quite how the DPA 1998 might be described as either a ‘side wind’ or not itself the will of Parliament – it was primary legislation enacted after an extensive process of debate and amendment – is not immediately apparent. Nonetheless, the decision of the IT was overturned and the Enforcement Notices all quashed.[210]

7.7 The aftermath of the *Five Constables* decision

The *Five Constables* judgment proved to be a decisive defeat for the Information Commissioner. Having acted to prevent the police from operating their compromise ‘step-down’ procedure, which he believed to be contrary to the DPA 1998 because it meant the deletion of too few criminal records even if records were ‘stepped-down’, he inadvertently invited an appellate court to decree that the police were not required to delete any records at all and that they did not need to step-down anything, either.[211] In short, the

[205] Ibid
[206] Ibid [42]
[207] Ibid [43]
[208] Ibid [107] (Hughes LJ)
[209] Above n.190 [44]
[210] Ibid [51]
[211] Ibid [3]

Commissioner was told that his complaint was entirely without merit; no more than a 'sidewind', in fact. Having brought his challenge to the public consciousness at the outset, his defeat was also played out in full public view. In the immediate aftermath of the *Five Constables* judgment, the ICO responded by effectively stonewalling it; making no comment to the media[212] and making no reference whatsoever to it in his subsequent annual report[213] (having previously cited with approval the IT decision which foreshadowed it).[214]

The police, meanwhile, were far more effusive. Ian Redhead, ACPO's Director of Information, told the media afterwards that 'the loss of such valuable information would have been detrimental to preventing crime and protecting the public'.[215] For the police, the judgment was a victory beyond any realistic expectation. Not only were they told they could retain all the data they had been ordered initially to delete but they were also told they didn't need to step anything down at all. In reality, the judgment provided the police was an absolute *carte blanche* 'to maintain all the records they thought necessary'.[216]

The decision, however, was met with widespread criticism elsewhere. Liberal Democrat MP Chris Huhne told the media that 'criminal convictions are of operational value to the police but it is hard to explain why keeping records of minor transgressions for 100 years is proportionate',[217] while Anna Fairclough, lawyer for *Liberty*, claimed that 'people will be forever haunted by the minor indiscretions of their youth…This judgment forgets the privacy rights of millions of people'.[218] Another civil liberties group, *Big Brother Watch*, described the decision as 'a criminal ruling on criminal records' and 'absolutely crazy'.[219]

Academic and practitioner comment was also largely critical. Anita Bapat noted that the case 'highlighted the potential detriment such retention may cause to individuals',[220] while

[212] See 'Police win data deletion appeal' *The BBC* (London, 19 October 2009) and 'Police win appeal to keep minor convictions on file' *The Guardian* (Manchester, 19 October 2009)
[213] Information Commissioner's Office, 'Information Commissioner's Annual Report 2009/10' (HC 220, 2010)
[214] Information Commissioner's Office, 'Annual Report 2007/08' (HC 670, 2008) 11
[215] 'Police win data deletion appeal' *The BBC* (London, 19 October 2009)
[216] D. Marshall and T. Thomas, *Privacy and Criminal Justice*, (Palgrave MacMillan, 2017) 123
[217] 'Police can keep records of minor convictions for 100 years' *The Telegraph* (London, 19 October 2009)
[218] D. Woods, 'Court ruling gives employers access to employee's criminal records' *Human Resources Magazine* (20 October 2009)
[219] A. Deane, 'A criminal ruling on criminal records' *Big Brother Watch* (19 October 2009)
[220] A. Bapat, 'The new rules on using children's data (1 May 2012) 12 (5) Privacy and Data Protection Journal 12

O'Connor claimed that while he agreed 'with the sentiment' that criminal records offered operational assistance to the police, 'surely there is another way [than 100-year retention]? Benefits to the police are minimal, but a huge cost to the individual…One can only hope that the legislature addresses the matter sooner rather than later'.[221] Treacy and Terlegas focused on the data implications, noting that the judgment offered data controllers the opportunity to provide upon ICO registration 'a wide range of processing activity, sometimes with only marginal relevance to the broadly stated purpose' which in turn means that the requirement that data be held for only lawful purposes provides 'only a limited check on the scope of data processing activities'.[222]

On 13 November 2009, almost a month after the *Five Constables* decision was handed down, the ICO finally broke their silence to announce that they intended to make an application for leave to appeal to the Supreme Court, claiming in a press release that the case:

> raises important issues not just for these and the many other individuals about whom very minor and aged conviction details are held but also about how the Data Protection Act 1998 is interpreted in practice. It also engages serious questions about the applicability of Article 8 of the European Convention on Human Rights to conviction data held by the police'.[223]

One academic noted that the latter was clearly 'a significant issue' and that many would 'watch the progress of the Commissioner's application with great interest'.[224] They would watch in vain: on 24 February 2010 the Supreme Court refused the application for leave to appeal.[225]

The Government, perhaps pre-empting an unfavourable determination in the *Five Constables* case which was not forthcoming, appointed Sunita Mason as their

[221] T. O'Connor, 'Does a recent decision mean some people will never escape past convictions?' (November 2009) Law Society Gazette < https://www.lawgazette.co.uk/law/-does-a-recent-decision-mean-some-people-will-never-escape-past-convictions/52936.article > accessed 23 May 2019
[222] B. Treacy and A. Terelgas, 'Under the spotlight: police retention of conviction data' (1 February 2010) 10 (3) Privacy and Data Protection Journal 12
[223] Information Commissioner's Office, 'Police cases: ICO's response to the Court of Appeal's judgment' (Press Release 13 November 2009)
[224] Above n.222, 13
[225] UKSC 2009/0204 (24 February 2010)

'Independent Advisor for Criminality Information Management' in September 2009.[226] Mason waited until after the decision in that case was made to commence her review, which was published in March 2010.[227] In this she recognised the 'strong views' that the police were the primary arbiters of what should be kept and for how long in the *Five Constables* case.[228] She then conducted a 'review' which showed that retention periods in other countries offered 'little consistency' in how long, and what, records were retained[229] and that there existed 'limited research and analysis that can be drawn upon which looks at the impact of differing retention periods on public protection arrangements'.[230] On this basis, and because the *Five Constables* decision has been based on 'information, evidence and statements from a range of sources',[231] Mason felt she did not have sufficient 'clear evidence' to depart from 'the steer provided by the Court of Appeal', and so recommended that all records be retained until the subject reaches 100 years of age.[232] She did also suggest that the Government may wish to conduct some research into the effectiveness of lengthy record retention on public protection issues.[233]

It is submitted that Mason's review was fundamentally flawed in a number of regards. The first is that, in accepting as the starting point the position taken by the Court of Appeal in the *Five Constables* case, Mason effectively exculpated herself of one of the most pressing of her terms of reference – namely to conduct an <u>independent</u> [author's emphasis] review into the policy of retention of record on the PNC.[234] An 'independent' review would not, it is submitted, ordinarily accept as a starting point and at face value the decision taken by the very arbiter which had given rise to the review being commissioned. In doing so, she likely got herself off on the wrong foot. This is further evidenced by her, it is submitted, inaccurate representation and analysis of the rationale of the Court of Appeal in the *Five Constable* case. It is difficult to see why she concluded that the Court in that case considered information and evidence from 'a range of sources'. As has been shown, that is simply not the case; the Court of Appeal instead accepted at face value the various assertions of serving police officers that the information had 'operational value', in spite of

[226] 'Home Office appoints crime data adviser', *The Guardian* (Manchester, 7 September 2009)
[227] S. Mason, 'A balanced approach: safeguarding the public through the fair and proportionate use of accurate criminal record information' (HO 01671 G, March 2010) 7, para.26
[228] Ibid, 5, para.12
[229] Ibid, 12, para.42
[230] Ibid, para.43
[231] Ibid, para.44.
[232] Ibid
[233] Above n.229
[234] Ibid, 30, para.2

their being unable to provide any detailed exposition or actual examples of how that manifested itself in practice.

Mason's review of the various detention periods in other EU countries also, it is submitted, provided her with an overly-simplistic analysis which rather befits her 'starting point'. Mason provides a tabulated summary of the retention periods in other EU countries at the time of her review.[235] While this does indeed show a lack of consistency across different countries and their respective retention periods, what is also clear is that the majority of other countries did not retain as much data, or for such lengthy periods, as that held on PHOENIX. Indeed, only seven[236] retained all criminality data for broadly comparably lengthy periods of time, though two of those countries which did retain all criminal convictions (Greece and Lithuania) deleted records earlier than 'death or at age 100 years' (81 and 75 years of age respectively).[237]

It is submitted that a more accurate analysis (or, at least, one alternative view to the 'inconsistent approach' analysis offered by Mason) of the comparative data showed that the retention policy for criminality data held on PHOENIX was, at that time, the joint most extensive in the European Union (in terms of what information was being held and how long it was held for). Indeed, of the other 26 countries surveyed, only five had comparably extensive retention policies to that of police in England and Wales; each of the other twenty-one nations either deleted some records, deleted all records after set periods or deleted records at an earlier age than those stored on PHOENIX. It is not entirely clear why Mason's review failed to comment on this obvious and, it is submitted, critical, differential and instead focused on there being 'a lack of consistency'.

As for Mason's inability to find any 'research or analysis' on how effective such lengthy retention might have on either police operational effectiveness or public protection, it is submitted that she might perhaps have considered the extremely lengthy, detailed and cogent research produced by Soothill and Francis which the Commissioner had put before the IT in opening the *Five Constables* litigation. Her report does not mention this at any point. It is arguably instructive that in commissioning her report, which bemoans a lack of

[235] Ibid at 36 – 41
[236] The seven comparable states are Cyprus, Czech Republic, France, Greece, Ireland, Lithuania and Slovakia.
[237] Above n.225, 38 – 39

research or analysis on this point, Mason's list of contributors[238] includes not a single academic or professional researcher; precisely the sort of contributors who might be able to have offered her some insight into that very pertinent issue. Indeed, her list of contributors is somewhat instructive generally: in order to complete her 'independent' review, she consulted no fewer than twenty-five senior police officers or other senior law enforcement officials and seventeen members of either the Home Office or other Governmental departments. It is not difficult to envisage the kind of input these 'contributors' were offering. By contrast, in addition to omitting entirely any academic input, only eleven charitable organisations were consulted, along with three members of the ICO.[239] It is submitted that such an imbalance legitimately calls into further question the 'independence' of her review.

Whatever the merits of Mason's review, the police had already pressed ahead. Waiting neither for Mason's review to conclude (and fully aware it was taking place as they were contributing to it), nor for the decision of the Supreme Court on the Commissioner's application to appeal the *Five Constables* judgment, the police formally abandoned their 'step-down' model and notice was sent to all chief constables that data would be retained, and used for all purposes, until death or the subject reached 100 years. This was sent just three days after the *Five Constables* decision was handed down.[240] The notice warned all chief constables not to step down any convictions and stated that the judgment 'in particular…confirms the power of the police service to retain conviction and caution data in the long term', entitles police to take a 'broad interpretation of the policing purposes' and that, in future, 'if any member of the public continues to query the retention of PNC records', they should be advised to write to the Information Compliance Unit'.[241]

Although the 'step-down' model was effectively defunct, and doubtless even less concerned than previously as to the interference of the Information Commissioner, no further formal guidance was administered regarding the retention of criminality data on the PNC until 19 March 2015 when the National Police Chief's Council ('the NPCC'), who had by this time replaced ACPO, issued a formal written policy for the retention and

[238] Above n.225, 33 – 35
[239] Ibid
[240] Ibid, 42
[241] ACPO, 'New Position on the retention of Police National Computer (PNC) Records' (22 October 2009)

deletion of criminal records held on the PNC ('the 2015 Policy').[242] So unconcerned were the police by data protection by this point that they effectively abandoned all pretence towards adhering to the DPA 1998: the phrase 'data protection' appears only once in the entire document (in a section confirming that chief officers remained Data Controllers)[243] while, for the first time, the NPCC did not even consult the Information Commissioner prior to drafting and issuing the 2015 Policy; indeed, the Commissioner was conspicuously absent even from the circulation list.[244]

The 2015 Policy confirmed that 'PNC records are retained until a person is deemed to have reached 100 years of age', and though a chief constable had a discretionary power to delete records, s/he must do so only 'in exceptional circumstances'.[245] Records would only be deleted if an individual requested it and persuaded the Chief Constable to do so. A prescribed form was provided for the individual applicant to outline the grounds upon which an application to delete was being made.[246] The individual was firstly required to meet the 'eligibility' criterion, outlined in Annex C of the 2015 Policy.[247] This provided that any conviction for any recordable offence would never be deleted, whether the individual was an adult or a child at the time of conviction, but that a person requesting the deletion of an 'out-of-court' disposal or an 'event history' record from the PNC met the 'eligibility' criterion.

That left the applicant with the requirement to make out a suitable 'ground' for deletion. These were set out in Annex A of the 2015 Policy. This provided that chief officers had the discretion to use their 'professional judgement' on whether to delete records or not. A requirement to decisions 'on balance of probabilities' or 'beyond all reasonable doubt' was expressly excluded.[248] No definition or guidance on what constituted 'professional judgement' was required and it is difficult to not see this as conferring an almost unfettered discretion on decisions to the chief officer. An exhaustive list of 'grounds' for deletion were then laid down. These included where a chief officer was satisfied that, after an investigation, no crime had actually taken place, that an allegation made had been done

[242] National Police Chief's Council, 'Deletion of Records from Police National Systems (PNC/NDNAD/IDENT1)' (v.1.1, 19 March 2015)
[243] Ibid, 4, para.1.6.4
[244] Ibid, preamble
[245] Ibid, 4, para.1.6.5
[246] Ibid, 9, para.5.2
[247] Ibid, 9, para 5.1
[248] Ibid, Annex A, para.1

falsely or maliciously, where the individual had established a proven alibi absolving them from an offence, where an individual was arrested as part of an incident but is later found to be a victim or a witness, rather than a suspect, where a judicial recommendation is made to delete the record, where an alternative person is subsequently found guilty of the same offence the individual was originally suspected of or where it was in the 'wider public interest' to delete the record.[249]

Once more, almost no guidance was provided as to when each of these might be made out, particularly the latter, which might potentially include a wide range of issues which were simply not highlighted in any significant manner. What was clear, though, was that record deletion would only be realistically considered if the individual to which the nominal record related could show 'positive evidence' that they had effectively been 'eliminated as a suspect' for the offence to which a record relates.[250] NFAs, for example, might be issued because a crime is found not to have taken place (in which case the record might be deleted upon request) or because the CPS believe there is insufficient evidence to charge the individual (in which case the individual remains a 'suspect', so the record will be retained).[251] Similarly, those acquitted at court or whose convictions are successfully appealed were not considered to be automatically 'eliminated as a suspect'; those acquitted because of insufficient evidence, for example, would likely have their data retained.[252]

7.8 Conclusions

For well over a century of criminality data collection by the police, there was a widely and publicly recognised acceptance by officers that criminal records lost operational importance as the record aged and where the record showed that the individual named was no longer committing further offences (or, at least, was no longer being convicted of them). Exceptions were made for those who committed the most grievous – sexual and violent – offences, but as such offences (and offenders) are rare, to all intents and purposes the principle of 'diminishing usefulness' was afforded general applicability and the police proactively deleted (or 'weeded') those records which were too old, too minor and too isolated to warrant retention for policing purposes.

[249] Ibid, para.3
[250] Ibid, 11, para.6.4.1
[251] Ibid, 10, para.6.1
[252] Ibid, para.6.2

The increased importance of, and implementation of legislation relating to, data protection, particularly requirements that data holdings must not be 'excessive' or held 'longer than necessary for stipulated purposes' might reasonably have been expected to ensure a tightening of the 'weeding' process; certainly, some MPs and the Data Protection Registrar/Information Commissioner thought so. Yet, by the 1990s, the opposite began to be evidence, and the police began to incrementally retract their position and instead elected to retain more and more records for longer periods. Exceptions to the 'diminishing usefulness' rule grew so that more and more records were retained and indeed formal guidance was issued by police chiefs to ensure consistency among forces. This occurred despite the police offering not a single piece of qualitative or empirical evidence to show that the general principal which had guided record deletion for over a century as having been proved to be incorrect. It is submitted that the introduction of the PNC, and particularly the creation of the PHOENIX application in 1995, must therefore have encouraged police forces to retain records at least in part because they now had the means to store and access them more readily.

Despite this, it was only after the *Soham* murders, and the subsequent public inquiry into them which found the police processed for the collation, retention and sharing of criminality data to be wholly inadequate, that the police abandoned their practice of deleting records and instead they elected to retain all records until each data subject reached age 100 years or died. This was done despite there still being no evidential or legislative basis for making such a determination; once more, nothing was offered by police to show that the general principal of 'diminishing usefulness' was misplaced, no statute passed mandated such a policy, there was no public clamour for such (and indeed many members of the public were so set against the policy that they sought redress from the ICO and the Courts) and no such recommendation was made to the police by *Bichard* either during or after his inquiry into *Soham*.[253]

The Information Commissioner, who had long considered the storage of criminality data on PHOENIX to be part of his remit, reacted by attempting to take the police to task. He

[253] The police actually retained records relating to Ian Huntley: the data failures highlighted in the Bichard Inquiry were not of record retention, but rather of record sharing between neighbouring forces holding local event histories which they hadn't added to PHOENIX as they should have. See C. Baldwin, 'The Vetting Epidemic in England and Wales (2017) 81 (6) Journal of Criminal Law 81 (6) 478, 489 – 491

was ultimately told that he was, in fact, mistaken. This was because he found an IT, and then later the Court of Appeal, willing to accept at face value the vague and unempirical evidence offered by police officers that these old records did, in fact and contrary to everything the police had said for decades, have an operational usefulness for the life of the subject. Moreover, he was ultimately undone by what in actuality amounted to little more than a 'throwaway' remark he himself made in evidence to the *Bichard* Inquiry, at the height of a media frenzy and public panic caused by an extraordinarily unpalatable, but mercifully rare, child abduction murder case.[254]

Since then, the Commissioner has retreated entirely from any policing role so far as criminal records are concerned, instead limiting the ICO contribution to poorly-disguised sniping from the side-lines, such as the lament presented to the NPCC in 2017:

> There are plenty of questions I feel police forces are still struggling to answer. Let's start with the retention of PNC records. Why are records being kept so long? It's a full year since my predecessor was asking in a foreword to this event how it could be proportionate for an arrest record to be held on PNC until an individual reaches 100 years of age. My view is no different. The law requires proportionality. That gives plenty of room for police forces to hold some data longer... But that does not mean that you can ignore data retention principles.[255]

Yet, as has been shown, that is precisely what the police are now doing. Given an effective *carte blanche* to do so by the decision in the *Five Constables* case, and with the ICO limited to making pleas to proportionality but lacking any realistic enforcement authority whatsoever, the police have returned to a position of holding a near unfettered discretion to ignore data protection so far as any limits on their criminality data holdings are concerned.

They have utilised that discretion to build an enormous repository of criminality data which now encompasses over twelve million individuals. They have abandoned the deletion of any records except in strictly limited circumstances far removed from those undertaken through their earlier weeding policies. They proactively now delete no PNC records. Only if a data subject applies for review will one be considered. And the number of review

[254] Ibid, 490 – 492
[255] E. Denham, Speech to the National Police Chiefs' Council Information Practitioner Event' (7 June 2017).

applications received are very small indeed: perhaps unsurprisingly, given the extremely limited circumstances in which a chief officer is able (or even likely) to exercise their discretion to delete. Indeed, the ACRO Criminal Records Office, which deals centrally with all PNC deletion requests, received just 4,216 applications for deletion between the implementation of the 2015 Policy and May 2018. Of these, just 1,208 saw records either partially or entirely deleted.[256]

It is submitted that the present situation regarding the near indefinite retention of criminality data, facilitated by the decision in the *Five Constables* case, is unjustifiable with regard to data protection principles and should be revisited. The reasons why the author believes this to be so are outlined at length in the remaining substantive chapters of this research.

[256] The data used to collate these numbers is available in the annual reports produced by ACRO: see ACRO Criminal Records Office, 'Annual Report 2015 – 16' (ACRO, 2016) 24, ACRO Criminal Records Office, 'Annual Report 2016 – 17' (ACRO, 2017) 20 and ACRO Criminal Records Office, 'Annual Report 2017 – 18' (ACRO, 2018) 13.

8
Justifications for revisiting the decision in the *Five Constables* case

8.1 Introduction

It is, at the time of writing, almost a decade since the decision in the *Five Constables* case. In the intervening period, and freed from the constraints of effective external oversight, the police controllers of PHOENIX have compiled an enormous repository of criminality information on their systems, encompassing over twelve million citizens.

The critical analysis which follows in this chapter aims to directly address the fourth research question. It is submitted that the passage of time has demonstrated that certain key elements of the court's reasoning in the *Five Constables* case are not correct, and that the common law principle set down by that case should now be reconsidered. Indeed, as will be seen, subsequent Supreme Court judgments have, by accident rather than design, already rendered significant passages of that judgment obsolete. This chapter will highlight these, along with other principles elucidated in the *Five Constables* case which, it is submitted, do not stand up to close scrutiny, including offering a critical evaluation of the police claims that the retention of old and minor criminality data aids in their operational processes and offering a brief comparison with the position on criminality data retention in Scotland.

8.2 The criminal justice system does not require a complete record

In the *Five Constables* case, Hughes LJ cited the use of criminality data on the PNC for sentencing purposes and for the credibility of witness as being part of the 'common coin' of the criminal court:

> the common coin of the criminal court depends upon access by the court, through the prosecution and thus through the PNC, to a reliable and comprehensive record of convictions and their circumstances...the criminal justice system thus depends on the maintenance of the PNC. If the PNC is not complete, the court can never know of a relevant old conviction.[1]

[1] [2009] EWCA Civ 1079 [109]

Indeed, this, said Waller LJ, was a 'complete answer' to the question of whether the data being held until the nominal record subject reaches 100 years of age was either 'excessive' or 'retained longer than is necessary' for the intended purpose.[2]

The truth is less straightforward that that overview suggests and has been examined at some length in chapter 4.4 of this research. It is not intended to reiterate that analysis here but it will simply perhaps suffice to state that criminal trials proceeded for centuries, on broadly comparable lines, while an incomplete antecedent record was retained and that even today there exists no express statutory requirement to retain a complete record of all convictions for any part of the criminal process. Moreover, while antecedents certainly do play an important role generally in the criminal process, it is submitted that there are no obvious (statutory or otherwise) reason why trivial and aged offences might be relevant to any charging decision, application for bail, hearing regarding 'character' evidence or a committal for sentence.

8.3 The 'Ian Huntley myth'

The century old policy of police to delete old records was never presumed to have caused any manifest injustice to anyone, nor to have contributed in any meaningful way to a failure of public protection, until in August 2002 two schoolgirls were abducted and murdered in the village of Soham by Ian Huntley.[3] Huntley's crime drew considerable public revulsion amidst an almost frenzied mass media coverage and his name, or alternatively simply 'Soham', has entered ordinary lexicography as an examples of what might go wrong when those disposed to commit extremely grievous acts are given an opportunity to do so in circumstances they should not have had.[4]

Over time, Huntley's crime has given rise to an emotive and largely erroneous narrative regarding the retention of criminality data which does not stand even the most basic scrutiny. Where that narrative is driven by the media, it is perhaps understandable, but it is submitted that where significant elements of it are repeated as fact by the judiciary, seeking to justify decision which allow for continued criminality data retention, it is

[2] Ibid [63]
[3] *R v Huntley (Ian Kevin)* [2005] EWHC 2083 (QB) [4]
[4] A full examination of the moral panic caused by Huntley's crime has already been conducted by this author elsewhere; see C. Baldwin, 'The Vetting Epidemic in England and Wales' (2017) 81 Journal of Criminal Law 478

inexcusable. Examples abound. One of the more common misconceptions is that *Soham* created the legislative regime for disclosing criminal records to third parties.[5] This is entirely false; the Police Act, which is provides the statutory basis for disclosing criminal records, was enacted in 1997 while the Criminal Records Bureau – the organisation tasked with dispensing criminal checks – opened in March 2002,[6] five months before Huntley committed his offences.

These inaccuracies even permeate the highest echelons of the judiciary. One is the notion that the two victims of Huntley's crimes were 'murdered by their school caretaker'.[7] This is also entirely false; the two murdered girls St Andrew's Church of England Primary School, while Huntley was employed at Soham Village College. He had no contact with his victims through his employment position, but instead through Maxine Carr, who worked at the primary school and who did know the two girls.[8] In fact, and contrary to common perception, Huntley did not know the two girls, nor they him.[9]

What makes these 'myths' damaging is that they, and indeed 'Soham' generally, are very often used to justify the present system of criminality data retention. Indeed, it is submitted that they are so often used, and in such emotive manner, that their use has become trite. The general proposition which emerges, perhaps best summarised by Baroness Hale, is that:

> We do not need any reminding, since the murder of two little girls by a school caretaker in Soham and the recommendations of the report of the Bichard Inquiry which followed, of the crucial role which piecing together different items of police intelligence can play in preventing as well as detecting crime.

The central tenets of this position are two-fold, and both, it is submitted, ill-founded. The first is that Ian Huntley was able to commit his crimes because the police were obligated by the DPA 1998 to delete data which might have otherwise have been retained and,

[5] Per MacGuire J in *Re: KC's application for Judicial Review* (26 February 2016) (QBD) unreported [11]
[6] C. Baldwin, The Demise of the Criminal Records Bureau' (2019) 83(3) Journal of Criminal Law 229
[7] Per Lord Sumpton in *Re: Gallagher, R(P) and two others v Secretary of State for Justice* [2019] UKSC 3 [75] and also J. Purshouse, 'Non-conviction disclosure as part of an enhanced criminal record certificate: assessing the legal framework from a fundamental human rights perspective' (2018) PL 668 at 679
[8] M. Bichard, The Bichard Inquiry Report, (22 June 2004), HC653, 24, paras 1.7 – 1.11
[9] Above n.3

therefore, they were unable to prevent him being employed as a school caretaker. This was addressed directly in the *Bichard* report, and found to be entirely incorrect. The inquiry found that Huntley had never been convicted of any offence but had come into contact with the police on eleven separate occasions between 1995 and 1999, including four sperate allegations of rape (one of which proceeded to Court, but not trial).[10]

It transpired that some of the contacts were not properly recorded.[11] In evidence, the Chief Constable of Humberside Police largely responsible for the missing records admitted in evidence to *Bichard* that 'he was unaware of the guidance or rules concerning when a record should be reviewed and when it should be deleted' and that he 'was unaware of the weeding rules and considered these a level of detail which he could not reasonably be expected to know'.[12]

That did not stop him attempting to blame the Information Commissioner and the DPA 1998 for the failure of police to record the contacts with Huntley or to utilise these to identify a possible pattern of offending which might give rise to a policing concern.[13] This, according to *Bichard*, was 'seriously misjudged'[14] and 'wrong'.[15] In fact, the Chief Constable later admitted to the Inquiry that 'the Information Commissioner's views on the issue had little or nothing to do with that information not being on the Humberside Police systems'.[16]

The wide dissemination by police of the notion that the DPA 1998 caused the deletion of records which resulted in Ian Huntley being able to commit murder[17] is, it is submitted, likely to have played a major part in its later, and continued, reiteration. It is, however, a myth. In truth, had the police not been committing repeated breaches of the DPA 1998[18] then they would have held accurate, up-to-date records on Huntley in accordance with the

[10] This author has elsewhere provided a detailed exposition of the findings of the *Bichard Inquiry* which explain why Ian Huntley was able to obtain a 'clear' criminal record check despite all of these police contacts; see C. Baldwin, 'The Vetting Epidemic in England and Wales' (2017) 81 Journal of Criminal Law 478, 488 – 491
[11] Ibid
[12] Above n.8, 96, para.2.105
[13] Ibid at 97, para.2.109
[14] Ibid, para.2.110
[15] Ibid, para.2.112
[16] Ibid
[17] Ibid, para.2.109
[18] As highlighted in Chapter 6.4 of this research

applicable Weeding Rules in force at that time which could have been utilised in an accurate criminal record check against his name

On no reading of the Weeding Rules in force at that time would such a pattern of behaviour, particularly one involving such serious allegations, have been deleted from the PNC; the allegations of rape alone should have been sufficient to allow all of the contacts with Huntley to be recorded and retained. The reason why records were not retained were rather, according to *Bichard*; inadequate training of staff, poor database maintenance, ineffective management, poor auditing and inefficient intelligence functioning.[19] These are police operational failings, not failings in the operational framework itself, and it was these police operational failings (described by *Bichard* as 'deeply shocking'[20]) which meant that the records were not available.

Very much linked to the myth that data protection resulted in the deletion of important police data is the proposition that 'the police stopped deleting records because *Bichard* said they should'; alluded to by Waller LJ in the *Five Constables* case.[21] This too is inaccurate. *Bichard* made thirty-one recommendations based on his investigation and not one of these suggested that the police stop deleting old, minor and inactive records. Eight of the recommendations did relate directly to either the PNC or to data management generally[22] but that most oft cited in that which recommends the police produce a 'clear, concise and practical' Code of Practice to replace the existing guidance on data retention[23] which should 'take into policing purposes and the rights of the individual and the law'.[24]

There is nothing, however, which says that the police should stop deleting records. Indeed, there is implicit acceptance throughout that records, or at least some of them, will still be deleted; the new code was expected to deal with 'record creation, retention, deletion [author's emphasis] and information sharing'.[25] Moreover, Bichard then went on to consider 'factors which should be taken into account in reaching retention or deletion decisions' in sexual offence matters.[26] He considered that the nature of the allegation,[27]

[19] Above n.8, 98, paras. 2.119 – 2.121
[20] Ibid, para.2.121
[21] Above n.1 [2]
[22] Above n.8, Recommendations 4 – 11, pp.13 – 14
[23] Ibid, Recommendation 8
[24] Ibid, 138
[25] Ibid, 135, para.4.43
[26] Ibid, 136, para.4.46
[27] Ibid, 136, para.4.46.1

the reliability of the allegation[28] and the age of the allegation[29] were all pertinent factors in determining how long a record should be retained before deletion. The last of these might be especially important, as an initial contact should be retained 'for a sufficiently long period for it to be seen whether a pattern emerges, even if that first allegation is to be judged at the lower end of the reliability scale'.[30] The Information Commissioner accepted these general policing principles but suggested that a retention period of more than ten years in this regard might give rise to data issues.[31]

All of this clearly implies that Bichard anticipated that at least some records would be deleted, even where these related to very serious offences. If Bichard had expected for the police to introduce a new code which essentially allows them to retain all records on PHOENIX (save the exceptional circumstances where an application to delete might be made), he would not, it is submitted, have taken the time to note factors to take into account when reaching 'retention or deletion decisions'.

Data protection did not cause the police to delete records they would have otherwise retained, nor did the inquiry convened order that the police stop deleting records. Ian Huntley did not commit his crimes because of data protection or record deletion; as Turner noted in 2009, 'it was pure mischance rather than the exploitation of an employment opportunity that landed the girls in his fateful company'.[32] The use of Soham as justification for the continued retention of criminality data on PHOENIX has become trite and does not stand close scrutiny. The myths are powerful and have persisted as time has passed. However, it is submitted that the time has come for them to be dispelled.

8.4 Why indefinite retention might be considered 'excessive'

In the *Five Constables* case, the police were offered the opportunity to explain in evidence precisely why old or minor criminality data was to be retained. Evidence was adduced which claimed that the convictions might be utilised to place a suspect in a geographical area at a period of time in a historical investigation or that these might in time reveal a pattern of criminal behaviour,[33] but these are theoretical examples and, as even Waller LJ

[28] Ibid, para.4.46.2
[29] Ibid, para.4.46.5
[30] Ibid
[31] Ibid, para.4.46.6
[32] A. Turner, 'Protecting Children Effectively' (2009) 173 Justice of the Peace 290
[33] Above n.1 [28]

conceded, 'that the information might be of value in certain circumstances and of value when taken together with other information'.[34]

There is a long-standing police assertion that criminal records assist them in preventing and detecting crime. If this is true, then the continued retention of criminality data cannot reasonably be considered 'excessive' for data protection purposes. However, it is not clear what evidence, if any, supports this contention other than the word of police officers who reiterate it as fact. The problem with such a position was expounded at length by Lord Kerr (albeit in a dissenting judgment in a case involving the retention of biometric criminality data):

> If we continue to define ex-offenders throughout their lives on the basis of their offending, we deprive them of reintegration into society on equal terms with their fellow citizens. The only reason proffered to justify the denial of that hope is the assertion that those convicted of offences may reoffend. The premise which must underlie this claim is that those convicted of recordable offences are more likely to reoffend than those who have not been. But no evidence has been presented to support that claim. Unsurprisingly, therefore, no attempt to quantify such a risk has been made.[35]

It is not easy to quantify the risk of former offenders committing further offences, but some indications which indicate that the usefulness of old and minor criminality data to policing purposes is far less than claimed will be considered below:

8.4.1 The back-record conversation programme was never completed

It will be recalled that, at the inception of the PHOENIX, PCL Group were contracted to input all of the paper records held by the NIB onto the computerised system.[36] PCL Group struggled almost immediately to convert the records at volume and the contract with them was terminated 'by mutual consent' in October 1996 with only 300,000 records converted.[37] Responsibility was transferred back to the Metropolitan Police,

---

[34] Ibid
[35] In *Re: Gaughran's Application for Judicial Review* [2015] UKSC 29 [95]
[36] Per ch.4.3 of this research
[37] 'PCL Loses Criminal Records Job', *Computing Online* (2 October 1996) <https://www.computing.co.uk/ctg/news/1835451/pcl-loses-criminal-records-job> (accessed 8 April 2019)

who added a further 200,000 records by 1999 but who soon-after effectively stopped converting the records, instead adding them on a 'come to notice basis', so that anyone who came to the attention of the criminal justice system would have their back record converted, while those who did not would not.[38]

Despite police claims that these old records are an invaluable resource to their operational processes, by August 2005, some 1.28 million records were still unconverted from microfiche.[39] Around the time that Waller LJ was accepting as fact the essential quality of old and inactive records for policing purposes in the *Five Constables* case, some 1,094,000 old (and presumably inactive) criminal records were still being held on microfiche and were not input onto the PNC, save by reference to a 'marker' which informed the PNC user that a microfiche record was held if required.[40]

By this time, comment on the 'back record conversation' process had effectively ended and it was not clear who was responsible for it or indeed whether it was still ongoing. Indeed, in the course of this research the only reference to be found to it was that provided by the ACRO Criminal Records Office in their annual reports, which indicate that they continue to convert some of the microfiche collection, albeit in very small numbers; in 2017/18, 4,626 records were added to the PNC.[41]

In the course of this research, investigations into the microfiche collection were conducted under the provisions of the Freedom of Information Act 2000. What these revealed is that in October 2012, at the authority of NPIA, these records, supposedly essential to the prevention and detection of crime, were transferred out of police hands and into storage by the Digital, Data and Technology Department of the Home Office, although Chief Constables remain the Data Controllers. While the ACRO Criminal Records Office 'provide a back-conversation service on behalf of some organisations', it remains unclear who, if anyone, is still otherwise actively engaged in converting the records. If someone is, then they do not appear to be making much progress; at April 2018, some 1,005,242 individuals with nominal listings on PHOENIX have no more information recorded other than a marker advising that a microfiche record exists

[38] T. Thomas, *Criminal Records: a database for the criminal justice system and beyond* (Palgrave MacMillan 2007) 37
[39] Ibid
[40] S. Mason, 'A Common Sense Approach: a review of the criminal record regime in England and Wales. Report on Phase 2' (Home Office 30 November 2011) 25
[41] ACRO Criminal Records Office, 'Annual Report 2017 – 2018' (2018) 1

relating to them. If police need to access the old data, a request is made to the 'Microfiche' team on a specified form.[42]

What these investigations indicate is that, so far as some one million or so data subjects are concerned, criminality data is being held by the police, and a nominal listing on PHOENIX made, relating to individuals who have been of no interest to the police, or the criminal justice system generally, whatsoever since, at the very latest, PHOENIX went live in 1995. These are individuals who have not 'come to notice' for at least twenty-three years. It is not clear, therefore, what 'operational use' this data has for policing purposes; indeed, the police have deemed this data sufficiently unimportant that they elected to transfer it to the Home Office, rather than retain it themselves. This appears entirely inconsistent with the premise that this type of data is essential for placing certain individuals in geographical areas or establishing patterns of criminality and it seems highly implausible to suggest that this data is helping in 'crime prevention'; the police do not even have ready access to it save completing and returning a specified form.

If, as appears to be the case, the vast majority of this data has little (or no) operational value, it is not clear why the holding of this data is not 'excessive' for the purposes of data protection legislation. It is, therefore, equally unclear why this data could not simply be deleted.

8.4.2 Scotland does not retain a complete collection

As has been show in the previous chapter of this research, the police themselves felt it unnecessary to retain certain criminal record data once it lost its operational value. This determination, based on the nature of the record itself and the length of time passed since the individual named came to the attention of the police, predated data protection legislation and was abandoned for reasons that the police have never properly explained.

[42] Home Office, 'FOI Request. Collection of historic microfiche criminal records' (FOI Case Ref: 49433 *What Do They Know?* 17 July 2018) <https://www.whatdotheyknow.com/request/collection_of_historic_microfich#incoming-1205670> accessed 8 April 2019

In the *Five Constables* case, Waller LJ placed considerable weight on his determination that the 1995 Directive[43] which ultimately resulted in the passing of the DPA 1998 permitted the state to collect a 'complete register of criminal convictions' as long as this was controlled by official authority.[44] This, he said, was sufficient to show that the PHOENIX collection was not excessive but was, instead, 'important'[45] in allowing the police to apprehend offenders and prevent crime.[46] He also claimed that the complete collection allowed for the CPS and courts to have access to 'the full information' required of them.[47]

If he is correct, and that a complete collection is required for all of these purposes, one wonder's what he would make of the system of criminal record retention in Scotland, where, in applying precisely the same European Directive, the same Parliamentary legislation relating to bad character, antecedents and court proceedings generally and where presumably police have a very similar understanding and approach to crime prevention and detection as colleagues in England, a markedly different approach is taken.

Scotland, like England, has a lengthy history of collecting criminality data and indeed the Scottish Criminal Record Office ('the SCRO') was formally opened in 1960.[48] Scotland, like England, implemented a centrally administered computer system for the collation, storage and retention of criminality data; in 1988 the 'Criminal History System' ('CHS') went 'live'[49] and remains the equivalent of PHOENIX for police in Scotland today. It is, like PHOENIX, intended as an investigatory tool, containing personal details and modus operandi details on suspects and offenders as mandatory data fields.[50] Markers for serious offenders, such as sex offenders, are added to nominal listings[51] and, also as is the case on PHOENIX, officers are trained to utilise the data as a crime

[43] See ch.6.2 of this research for a detailed examination of this.
[44] Art 8(5) of the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995
[45] Above n.1 [9]
[46] Ibid [48]
[47] Ibid
[48] Above n.38, 24
[49] 'Report of the Working Group on the Recording and Weeding Policy for the Criminal History System' (Scottish Criminal Record Office 2004) 4, para.1.5
[50] Scottish Parliament, 'Justice 2 Sub-Committee: Child Sex Offenders Inquiry' (HMSO 3 October 2006) 33
[51] Ibid, 29

prevention tool, to conduct searches on suspicious individuals giving rise to concern for officers on patrol, for example.[52]

Unlike PHOENIX, however, CHS makes no distinction between 'recordable' and non-recordable offences; there is no such distinction in Scottish law so all offences are recorded to CHS.[53] Crucially, however and unlike PHOENIX, Scottish police weed data from CHS. In November 2001, the SCRO established a 'Recording and Weeding Group' to examine aligning a retention and weeding policy with that in force for the PNC. That group recommended that an alignment be made but it's report was never submitted to the Scottish equivalent of ACPO because of the tumult which began to envelop criminal records in England and Wales, outlined in the previous chapter. [54]Instead, the group elected to suspend all future meetings and wait for matters to settle in England and Wales, before recommencing their review in October 2004.[55]

The Group noted that 'the feeling in ACPO is that the weed policy for PNC should change to retention policy for all information; i.e. weed nothing' and that this 'was being met with a certain level of resistance by both the Home Office and Information Commissioner'.[56] Noting that the Scottish executive had 'intimated' that they did not necessarily intend to follow England's lead, the Group concluded that it would be best to 'continue to monitor the situation in England and Wales to identify any benefits or conflicts for Scotland' because the Group could 'see no possibility at this time of aligning the weeding policy of the CHS with that of the PNC'. Therefore, it recommended that 'SCRO does NOT [original emphasis] align its weeding policy with that of the PNC at the present time'.[57]

It seems clear that SCRO were, at that time, concerned to balance policing operational requirements against the perceived threat of enforcement action by the Information Commissioner; indeed, the Group warned data must be held for a proportionate time to facilitate policing purposes and not be excessive and that the IC had begun to take action against English police forces for excessive data held on the PNC.[58]

[52] Ibid, 30
[53] Above n.49, 3, paras.1.2 – 1.4
[54] Ibid, 6, para.2.1
[55] Ibid, para.2.2
[56] Ibid, 6 – 7, para.2.2
[57] Ibid, 12, para. 3.5
[58] Ibid, para.3.6

Even when that threat passed, through *Bichard a*nd the *Five Constables* case, police in Scotland resisted the opportunity to align their retention policies with forces in England. A policy document was drafted in February 2011 which approved the recommendations of the SCRO Group.[59] This resulted in the intimation on 23 November 2011[60] of what was (and indeed still largely is), by any measure and certainly by comparison to the weeding and step-down guidance previously produced by ACPO in England, a remarkably straightforward policy for the weeding of criminality data. This document has undergone four revisions (at the time of writing) and the current version was published 2 August 2018.[61]

The guidance for the storage and retention of criminality data in CHS contrasts sharply with that offered by the NPCC for PHOENIX. It opens with an affirmation that Data Protection has been considered and that the document is considered complaint with those obligations.[62] Like PHOENIX, a nominal listing is created on CHS whenever a case investigation is opened. However, unlike PHOENIX where police create an 'event history' which is almost always retained until the data subject reaches age 100, new listings on CHS are marked as 'pending'[63] and, where the case to which the listing relates results in a 'non-finding of guilt' of the data subject (NFA, discontinuance, acquittal etc.), the data is re-marked 'temporary retention'[64] and is thereafter automatically weeded after six months[65] unless the case involved a sexual or serious violent offence, in which case the files are automatically weeded after three years.[66]

Two notes should be made at this point; firstly, 'weeded' takes the old meaning, in that the data is deleted (i.e. 'completely removed')[67] from CHS, not 'stepped-down' for police eyes only, and, secondly, that CHS has an automatic deletion function. Unlike

[59] Association of Chief Police Officers Scotland (ACPOS), 'Recommended Record Retention Periods' (February 2011) 104 at s.(1)
[60] Association of Chief Police Officers Scotland (ACPOS), 'Recording, Weeding and Retention of Information on Criminal History System – Guidance' (v.1.0, 23 November 2011)
[61] Police Scotland, 'Recording, Weeding and Retention of Information on Criminal History System – Guidance' (v.4.0, 2 August 2018)
[62] Ibid, 4, para.1.1
[63] Ibid, para.1.2
[64] Ibid, para.1.4
[65] Ibid, 6, para.7.1
[66] Ibid, para.5.2
[67] Safer Scotland, 'Discussion paper on the Rehabilitation of Offenders Act 1974' (APS Group Scotland August 2013) 22

PHOENIX, which requires human input to ensure review and deletion, CHS simply deletes the data when the requisite time elapses. Such a system ensures that no data is retained which should not be and will evidently reduce the administrative burden on police forces to manually review and weed data – one of the various reasons cited by police in England for their historical failures to weed PHOENIX in accordance with their own policies.

As regards other disposals, there are once more considerable discrepancies in approach between CHS and PHOENIX. While in England and Wales there is a starting point which presumes that all conviction data will be retained until the subject is aged 100 years or dies, in Scotland the starting point[68] is that where a data subject reaches aged 40 years, a court conviction will be weeded if twenty years have passed since the conviction. If the data subject reaches aged 40 but the conviction is more recent than twenty years, the conviction is retained until twenty years pass and it is then automatically weeded. This is the so-called '40/20 rule'.[69] There are limited exceptions for 'higher-level offending', which provide that convictions on indictment, those disposed under the Mental Health Act or where a sentence of imprisonment is imposed[70] are all subject to retention until the subject reaches aged 70 and thirty years have passed since the conviction; the so-called '70/30 rule'.[71] Again, once both conditions are met, CHS will perform an automated weed of the data and it is deleted.[72] Only where a data subject is given a life sentence, detained at Her Majesty's pleasure, given an indeterminate sentence or where the conviction is a sexual or sexually aggravated offence is a CHS record to be retained for the life of the data subject or until the subject reaches aged 100 years.[73] Sexual offences were originally categorised within the 70/30 rule but were recategorized in 2013 after the police considered evidence which showed that 1.5% of enhanced disclosure checks in Scotland related to the over-70s.[74]

[68] Above n.61, 4, para.2.2
[69] Ibid, 4, para.2.1
[70] Ibid, 5, para.3.2
[71] Ibid, para.3.1
[72] Ibid
[73] Ibid, para.4
[74] Police Scotland, 'Recording, Weeding and Retention of Information on Criminal History System – Guidance (v.2.0, 6 June 2013) 4, para.4. As this group will have mostly retired from work, presumably these enhanced checks related to applications for voluntary positions, which would likely explain the police safeguarding concerns. 'Enhanced checks' are dealt at ch.8.5, below.

Other CHS weeding provisions offer stark comparisons to PHOENIX retention principles. While police cautions are recorded on PHOENIX until the data subject dies or reaches age 100, the Scottish equivalent – the 'police warning' – is only retained on CHS for two years from the date of insertion. The same retention period, and therefore the same comparison, applies in respect of the Fixed Penalty Notices – the Scotland equivalent of PNDs.[75] An entirely different approach to juvenile offending is taken in Scotland as compared to England; rather than prosecution, children are instead diverted to a system of 'Children's Hearings' which take place largely outwith the Court system.[76] This means that the majority of juvenile offenders are not formally convicted by a court but rather a finding is made by a tribunal at a Children's Hearing. Where this occurs, it is recorded on CHS and then weeded two years after insertion,[77] unless the record relates to a sexual or serious violence offence, in which case they are retained for three years and then reviewed. If not manually deleted, the record is reviewed annually thereafter until (or unless) it is deleted.[78]

The contrast between the approach taken in Scotland and in England is very stark indeed. What is intriguing about the Scottish system is that it provides for police retention of varying categories and types of criminality data for differing periods based on a simple approach to determining what might be proportionate or excessive. It uses the criminal justice system itself as the principal demarcation points. It accepts that data relating to those who are not convicted should not be retained for a lengthy period because those who are not convicted should not be treated the same as those who are – a notion considered in considerable length in the next chapter of this research.

It then uses the criminal justice system itself as a metric against which proportionality can be measured, so that non-court disposals, which by their nature indicate a very low level of criminality (alleged or otherwise) are retained for the shortest period, while court disposals are themselves subcategorised in accordance with the seriousness of the offence as determined by the criminal justice system. Crimes on indictment are more serious than summary offences, so data relating to these should be retained longer and doing so is more proportionate. Offenders who receive custodial sentences have committed more serious offences than those who commit summary offences, so data

[75] Above n.61, 5, para.5.1
[76] These are broadly outlined in Pt.1 of the Children's Hearing's (Scotland) Act 2011
[77] Above n.75
[78] Above n.61, 6, para. 5.3

relating to these should be retained longer and doing so is more proportionate. There is a greater need to protect the public from violent and sexual offenders than others offenders, so data relating to these should be retained longer and doing so is more proportionate.

Although in themselves not evidence based, the principles which underpin the Scottish approach to CHS are neither discretionary nor subjective. They do not require an evaluation of matters by a chief officer or indeed anyone else. They are instead a set of inherently simple, universally accepted notions which underpin the criminal justice system in both Scotland and England, articulated clearly and utilised to create a straightforward policy for data retention and deletion which is clear, logical and, it is submitted, a significantly more proportionate (and data protection compliant) approach than the blanket approach offered by the NPCC in respect of PHOENIX.

It is not clear why the extensive retention of minor and aged criminality data considered an essential part of operational intelligence underpinning crime prevention and detection in England and Wales, as is routinely claimed by chief officers and accepted in the *Five Constables* case, but such data is considered sufficiently unimportant by chief officers ten miles north of Berwick that they feel it appropriate to simply delete it from their systems after a sufficiently lengthy period of time passes.

If *Soham* is the justification for that divergence of practice, then it must be a fundamentally weak one, because Scotland has not, to this author's knowledge, suffered a deluge of Ian Huntley-type offenders infiltrating schools and murdering school-children. Indeed, it is difficult to see the crime prevention and detection justification carrying much weight at all. Whilst accepting that direct and detailed statistical comparison is fraught with difficulty,[79] the most recent official data suggests that, in Scotland, recorded crime is at its second lowest level since 1974,[80] homicides are at their lowest levels since 1976,[81] crime levels overall have 'been on a downward

[79] This is because the two jurisdictions have, among other things, different means of measuring crime rates, disposals, clear-up rates and indeed differing crime survey questions; for a fuller examination of the inherent difficulties of such an approach, see P. Norris and J. Palmer, 'Comparability of the Crime Surveys in the UK: a comparison of victimisation and technical details' (2010) Scottish Centre for Crime and Justice Research. This is before sociological and economic factors are considered, which will also inevitably influence crime statistics.
[80] National Statistics (Scotland), 'Recorded Crime in Scotland, 2017 – 18' (25 September 2018) 1
[81] 'Scottish homicides at lowest level since 1976', *The BBC* (London, 30 October 2018)

trend'[82] and that fear of crime in Scotland is at its lowest level since records began.[83] Police 'clear-up' rates for recorded crime[84] were 49.5%.[85]

In England and Wales, meanwhile, recorded crime increased by 7% between 2017 – 18, homicide rates increased by 14% in the same period[86] and have been on an upward trend since 2014, as has recorded crime generally.[87] One *Ipsos Mori* poll found that fear of crime is now one of the most important concerns of citizens in England and Wales and indeed the most pressing concern for Londoners[88] while official statistics showed that police forces were closing investigations after having identified no suspect in 48% of crimes reported to them.[89] It is perhaps not surprising, therefore, that the chairman of the Police Federation told the BBC in January 2019 that 'society just isn't as safe as it once was'.[90]

It is not clear whether this apparent divergence between fear of crime, recorded crime levels and crime detection rates in Scotland as compared to England and Wales has anything to do with the respective collation, retention and use of criminal records by police forces in each jurisdiction. What can be seen is merely that crime rates are rising and undetected offences remain high even though the police are collecting and retaining more data on PHOENIX than ever before.

8.4.3 Recidivism studies support the deletion of old, inactive records.

The most commonly cited justification for the police retention of criminal records in an operational sense is based predominantly upon the presumption that previous criminal convictions are a valid predictor of future criminal behaviour. Indeed; 'there is strong evidence that individuals with a criminal history are more likely to commit future crimes than individuals with no criminal history'.[91]

---

[82] Above n.80, 12
[83] 'Scots feel safer than ever before', *The BBC* (London, 27 March 2018)
[84] A definition of what constitutes a 'clear-up rate' is provided at above n.80, 67
[85] Ibid, 3
[86] 'Crime figures: Violent Crime recorded by polices rises by 19%', *The BBC* (London, 24 January 2019)
[87] M. Weaver, 'Homicides in England and Wales rise by 14%', *The Guardian* (London, 24 January 2019)
[88] R. Wright, 'UK fears over rising crime muddied by contradictory statistics' *The Financial Times* (London, 8 August 2018)
[89] Home Office, 'Statistical News Release: Crime Outcomes in England and Wales, year ending March 2018' (19 July 2018)
[90] Above n.86
[91] R. Karl Hanson, 'Long-term recidivism studies show that desistance is the norm' (9 September 2018) 45(9) Criminal Justice and Behaviour 1340

This ‘strong evidence’ is ordinarily taken from academic studies into reoffending (or ‘recidivism’). Recidivism, taken from the Latin *recidere* (‘to fall back’) is the trait of offenders who, having been convicted of an offence; ‘are not rehabilitated. Instead, he or she falls back, or relapses, into former behaviour patterns and commits more crimes’.[92] Recidivism is a widely researched academic discipline, and it is not the intention of this research to duplicate or add to the existing literature on it. Rather, what follows is a (very) brief summary of some of the key issues as might pertain to the notion that criminal records data should be retained as it is on PHEONIX as it will assist in the prevention and detection of crime.

The general starting point is perhaps that there is a wealth of data which suggests that a significant proportion of those who are convicted of an offence are soon-after convicted of another offence. This is particularly noticeable so far as those convicted and imprisoned as a result are concerned and various figures for this group are available and appear relatively stable over time; a study in 1995 found recidivism rates of 58% among the study sample within a two year period,[93] while another in 2016 suggests that ‘around 50% of prisoners go on to reoffend within one year of being released’.[94]

Even where the subject group is expanded to include ‘low-level’ offenders who commit offences but are not imprisoned, the re-offending rates remain high. The Ministry of Justice produces quarterly statistics on ‘proven re-offending’ rates which show that the rate of individuals handed a court conviction or caution one year or less after having received an earlier court conviction or caution fluctuated between 29 – 32% since statistics started to be collated in 2009.[95] Moreover, there is a general suggestion among the studies that ‘many offenders are generalists when it comes to committing crimes’.[96] The position was summarised by Redmayne as being that:

[92] M.D .Malz, *Recidivism* (Academic Press Inc, Florida 2001) 54
[93] C. Kershaw, J. Goodman, and S. White, *Reconvictions of Offenders Sentenced or Discharged from Prison in 1995, England and Wales*, (HOSB 19/99, London 1999) Table 2
[94] N. Booth, ‘Prisoners’ families and children’ (2017) 181 Justice of the Peace 246
[95] Ministry of Justice, ‘Proven Re-offending statistics Quarterly Bulletin, January 2017 to March 2017’ (31 January 2019) 1
[96] R. Lippke, ‘Criminal record, character evidence and the criminal trial’ (2008) 14(3) Legal Theory 167, 174

> Previous offenders—whatever their offence—are more likely to steal than are members of the general population; this holds for just about any offence. This affirms what we know from other sources: criminals tend not to be narrow specialists but have a general propensity to commit crime.[97]

This trait is often referred to as 'propensity'.[98] One landmark study conducted by Redmayne calculated that the propensity rates within two years of last conviction for various offences (with a custodial sentence imposed) ranged from 36 times more likely than those without any conviction for drug-related offences, 80 times more likely for sexual offences up to 125 times more likely for robbery offences. Where a non-custodial disposal is made, the propensity figures increase significantly for sexual offences and robberies, up to 250 and 400 times more likely respectively.[99]

It is the propensity of offenders to reoffend that gave rise to the introduction of 'propensity' evidence in the context of bad character applications at trial. It is also the justification police cite when arguing that a collection of criminality data is essential in allowing them to prevent crime (by monitoring known offenders who have a propensity towards committing offences) and to detect crime (by identifying suspects from a pool of individuals with a known propensity for committing offences).

Taken at face value, the tenets which emerge from these studies appear to give rise to a strong argument that the retention of data on PHOENIX for police operational purposes cannot be 'excessive' on any measure, let alone so far as data protection is concerned. However, it is submitted that taking these studies at face value is an erroneous proposition for a number of reasons. The first is that the argument in favour of retention must accept that the police actually utilise the data for closely monitoring known offenders and crime detection purposes. Indeed, many forces do not use the PHOENIX collection as 'intelligence' at all and there is considerable evidence to show that the police simply see criminal records collection as a repository of administrative data.[100]

---

[97] M. Redmayne, 'The relevance of bad character' [2002] 61 The Cambridge Law Journal 684, 697 – 98
[98] Ibid, 692
[99] Ibid, 695
[100] As outlined at length at ch.4.2, ch.4.3 and ch.6.4 of this research.

That notwithstanding, even the empirical data itself is subject to considerable question. Studies on recidivism are naturally based on 'known' offenders and 'known' offending. It is widely accepted that significant proportions of total criminality are not reported to the police, that significant proportions of crime reported go unsolved and that significant numbers of 'resolved' crime does not lead to a conviction. Even Redmayne concedes that his studies relate to 'convictions', rather than 'commissions' of crime[101] and that, therefore, his propensity figures must be treated 'with a degree of scepticism'.[102]

Even putting aside the empirical concerns, the very nature of policing and the introduction of propensity evidence in the criminal justice system means that supposed propensity traits must be evaluated with a very critical eye. For those police forces who do use PHOENIX data as an investigatory tool, it is difficult to see how useful it can be other than to provide a 'pool' of possible suspects in a reactive police investigation.

The potential problem here is obvious; such an approach inevitably leads the police to 'round up the usual suspects' in the hope that one will yield a successful clear-up. There is little question that such an approach is broadly taken by the police; Gill found precisely this approach being taken when he studied two police forces in the 1990s and commented that the preferred investigative method generally consisted of police officers deciding; "Oh I know who it is, it's Joe Bloggs, he's bang at it … that's one of the favourite sayings, he's bang out, he's well at it…'[103] Another study saw a police officer admit that 'the whole intelligence led process can be corrupted by the banter that goes on and the self-fulfilling prophecy. You know that someone can become a [target] because everybody talks about them, and then we start targeting them and because we target them they become something that they are not'.[104] Statisticians and analysts hired by police forces are often derived, with one reportedly told by an experienced officer conducting an investigation that 'it's all right you sitting there but you don't have a nose for what's going on'.[105]

[101] Above n.97, 700 – 701
[102] Ibid, 701
[103] P. Gill, *Rounding up the Usual Suspects? Developments in Contemporary Law Enforcement Intelligence* (Aldershot, Ashgate 2000) cited in N. Cope, 'Intelligence-led policing or Policing-led intelligence'? (2004) 44(2) British Journal of Criminology 188, 199
[104] N. Cope, 'Intelligence-led policing or Policing-led intelligence'? (2004) 44(2) British Journal of Criminology 188, 199 – 200
[105] Ibid

It is not even in reactive police investigations that this 'usual suspects approach' takes place and is likely to skew general propensity figures towards showing something that might not necessarily be as prevalent as claimed. There is evidence to show that, where PHOENIX data is used at all by police to help prevent crime, this is done by police focusing resources on 'target groups', such as those with previous convictions, who are likely to yield 'results'.[106] This will inevitably mean that those with previous convictions are more likely to find themselves caught committing offences than those without prior convictions, who might still be committing offences but are not being watched.

Even beyond policing itself, the use of propensity in the criminal justice system might well have an adverse impact on the data upon which it is based. The admittance of bad character evidence at trial has an obvious potential to bring to trial cases which are, in themselves, inherently weak but which might 'get over the line' where propensity evidence is adduced.[107] There are other reasons why individuals with criminal records might be more readily convicted. The CPS might be more prepared to prosecute 'known offenders' than those who are not.[108] Some defence lawyers might not pursue the defence of their client with particular vigour if they know their clients have previous convictions, particularly of a 'similar' type; this has been referred to as lawyers taking a 'presumption of guilt' approach.[109]

Darbyshire, meanwhile, in several studies of practice in the magistrates court highlighted what she saw as a significant problem regarding 'the regulars and their friends and family'.[110] She saw that each court 'had a hard core of regulars, who were often part of large extended families and/or gangs of friends'[111] which meant that magistrates inevitably became familiar with them. This led to entire family names, and those associated with them, become 'notorious' among benches as 'persistent offenders'; one clerk in Nottingham told her that:

---

[106] D. Farrington, 'Official bias in Intergenerational Transmission of Criminal Behaviour' (2013) 53(3) British Journal of Criminology 438, 451
[107] R. Munday, 'Round up the usual suspects! Or what we have to fear from Part 11 of the Criminal Justice Act 2003' (2005) 169 Justice of the Peace 328
[108] Above n.102
[109] M. McConville, J. Hodgson, L. Bridges and A. Pavlovic, *Standing Accused: The Organisation and Practices of Criminal Defence Lawyers in Britain* (Clarendon Press, Oxford 1994) ch.6
[110] P. Darbyshire, 'The Law Commission Consultation Paper on previous misconduct; Part 3: Previous Misconduct and magistrates courts – some tales from the real world' (Feb. 1997) Criminal Law Review 105, 106
[111] Ibid

> If your name is Bane or Pain in Nottingham, then you're notorious. Some of them have changed their name by deed poll. The Banes and the Pains provide a lot of work for this court and everybody knows them. If it's a problem at this court, the biggest Bench in the country, with over 450 justices, then it could be a problem anywhere.[112]

It is not difficult, therefore, to suppose that the notion of 'criminal propensity' as a general position may over-exaggerated in the bare empirical which if oft cited to support it. If the police use this as a means of focusing resources towards 'suspect groups', then it is hardly surprising that these individuals are caught committing more offences than those who are not so 'targeted', so are convicted more often. If the police investigate crime by rounding up a pool of 'usual suspects', it is hardly surprising that these individuals are more liable to conviction than those who are not. Equally, it is not difficult to image how more liable to conviction an individual might be if magistrates are considering particular family groups 'notorious'.

None of this is to say that these individuals are not committing offences. They may well be. The criticism here is that they are more likely to be convicted (or cautioned) than those who do not have criminal records because they are more likely to be caught, more likely to be prosecuted and more likely to be found guilty than the unconvicted who are not being so subjected to the criminal justice system. This is important because it is precisely with this group that comparisons are being drawn. It has led to come claiming that 'criminal propensity' has become a 'self-fulfilling prophesy' based on 'nothing more substantial than the prejudices of the criminal justice system'.[113] While an extreme view, it is submitted that the idea is not without merit and must be taken into account when analysing the usefulness, or otherwise, of the PHOENIX collection.

Even if it is accepted that criminal propensity is a genuine and measurable trait, and that this justifies the extensive collection of criminality data by the police because it allows them assistance in preventing and detecting crime (where it is even properly used for such purposes), then there remain three key caveats which, it is submitted, offer empirical support for the proposition that at least some of the nominal listings on

[112] Ibid, 107. The real family names in question were changed in the original research.
[113] Per S. Box, *The Criminal Justice System and Problem Populations*, cited in N. Lacey, *A reader in Criminal Justice* (Oxford University Press 1994) 36 – 62

PHOENIX offer such a disproportionately small benefit in this regard that their holding until the data subject reaches aged 100 years is 'excessive' on any interpretation of that term, and certainly as regards data protection legislation.

The first that there is a widely accepted, empirical acceptance that juveniles and young adults are a special category of offender to whom ordinary principles might not apply. This is because of two key, measurable and correlating factors. The first is that juveniles historically commit a disproportionately high volume of offences. One Home Office self-reporting study in 1995 found that one in two males aged 14 – 25 admitted to having committed one or more offences,[114] while another Home Office paper published in 2012 used the PHOENIX repository to conduct a statistical analysis which concluded that young people aged between 10 – 17 years had in 2009/10 committed around 1.01 million offences; 23% of the total number of offences recorded.[115]

Young people have a disproportionate tendency towards 'acquisitive offences', such as shoplifting, robbery and offences against vehicles, and offences of criminal damage.[116] They are also far more likely to be reconvicted than adult offenders. The most recent Ministry of Justice statistics show that, while 28.1% of adult offenders were reconvicted within a year,[117] 39.9% of juvenile offenders were reconvicted in the same period.[118] This trend has been borne out in countless studies of recidivism in juveniles and is marked regardless of offence severity or disposal; an Audit Commission study in 1996 found that 60% of those arrested by police on suspicion of an offence had at least one prior warning or caution[119] while another study in 1998 found that 28% of those issued police cautions were either cautioned again or convicted in court over a five year period.[120] In 2017, 28.3% of juvenile issued cautions were proven to have reoffended within one year.[121]

[114] J. Graham and B. Bowling, 'Young People and Crime' (Home Office Research Study 145, 1995) X
[115] C. Cooper and C. Roe, 'An estimate of youth crime in England and Wales' (Home Office Research Report 64, May 2012) 4
[116] Ibid, 8
[117] Above n.95, 4
[118] Ibid, 6
[119] Audit Commission, 'Misspent Youth: Young People and Crime' (1996) 2
[120] C. Nuttall, P. Goldblatt and C. Lewis, 'Reducing Offending: An assessment of Research Evidence on ways of dealing with Offending Behaviour' (Home Office Research, Development and Statistics Directorate, 1998) 86
[121] Above n.95, 8

The reoffending rates where a custodial disposal is given are very high indeed; a 1997 Government study found that 84% of 14 – 17 year olds released from custody were reconvicted within two years,[122] while in 2011 – 12, juveniles released from custody had a proven reoffending rate within one year of 72.6%.[123] A comparable data study in 2017 showed the rate to be only slightly less at 68.2%.[124]

The net result is that juvenile and young adult disposals form a significant proportion of the PHOENIX collection. Moreover, most of the nominal listings will have been created during the data subject's youth – 'adult-onset' offending is comparatively unusual; around 70% of all offenders start their offending behaviour as juveniles and those who engage in 'adult-onset' offending tend to do commit different types of offences, such as sex offences, thefts from work and fraud[125] – and very many will include multiple disposals; statistically, juveniles who are reconvicted tend to be reconvicted for more than one offence; in 2017 the average number of offences committed by reconvicted children and juveniles was 3.92.[126]

However, so far as the retention of these records for operational policing purposes is concerned, some discernible and distinctive patterns of criminality among offenders then emerge. The first is that there is a generally accepted starting point that there is a statistically increased probability that an individual convicted of an offence is likely to commit a further offence. The probability is greater in males than females, but very high in both, even if the individual has only committed one previous offence.[127] One of the ultimate extensions of this proposition is that a number of offenders ultimately become recidivistic offenders and commit a disproportionately large number of offences; a Ministry of Justice analysis of PHOENIX in 2010 found that 18% of juveniles convicted of first offence in 2000 went on to be reconvicted of ten or more offences by 2009,[128] while the Home Office has previously claimed that some 5,000 recidivists commit 10%

[122] Social Exclusions Unit, 'Reducing re-offending by ex-prisoners' (The Office of the Deputy Prime Minister, July 2002) 155
[123] R. Arthur, 'The Criminal Justice and Courts Act 2015 – Secure Colleges and the Legitimation of State Sponsored Violence' (2016) 79(1) Modern Law Review 102 – 121, 118
[124] Above n.118
[125] T. R. McGee and D. P . Farrington, 'Are there any true adult-onset offenders?' (2010) 50(3) British Journal of Criminology 530, 549
[126] Ministry of Justice, 'Youth Justice Statistics 2017/18 England and Wales' (31 January 2019) 61
[127] M. Vere van Koppen, 'Criminal Career Dimensions of juvenile and adult-onset offenders' (March 2018) 4(1) Journal of Development and Life-Course Criminology 92 – 119
[128] Ministry of Justice, 'The Youth Justice System in England and Wales': reducing offending by young people' (HC 663, 10 December 2010) 15

of all crime, and that 100,000 persistent offenders commit half of all recorded offences.[129]

So far as these individuals are concerned, the retention of criminality data might logically assist the police in an operational sense. These are active offenders and the police might reasonably need access to an extensive repository of criminality data to assist them in identifying where these offenders are most likely to offend, how they are likely to commit offences and what type of offence is likely to be committed by that offenders. Properly used, such data might allow for persistent offenders to be monitored by police or apprehended after having committed offences.

However, the number of such persistent offenders is very small and, by contrast, almost all other offenders eventually 'desist'. Desistance is 'the long-term abstinence from criminal behaviour among those for whom offending had become a pattern of behaviour'[130] and is far more common than might be imagined; indeed, Farmer et al simply state that 'there is no longer any debate in the field that criminality is a pattern of behaviour from which most individuals eventually desist'.[131] Some general desistance trends are equally well recognised. The first is that offending behaviour tends to peak very early in life. Individual studies offer different ages for 'peak' levels of offending, but these almost always point to an early age – some claim an age of sixteen,[132] others seventeen[133] and others eighteen[134] - after which point offending almost always decreases markedly. This is referred to by criminologists as the 'age-crime curve' and is universally recognised as a criminological constant; Manuna claims that 'one of the few near certainties in criminal justice is that for most people, offending

[129] See ch.4.2 of this research for a detailed evaluation of this, though the claims should best be taken with a large pinch of salt; see R. Garside, 'Crime, persistent offenders and the justice gap' (Crime and Society Foundation, October 2004) 14 for a full critical evaluation of the likely veracity of such claims.
[130] F. McNeil, S. Farrall, C. Lightowler and S. Maruna, 'How and why people stop offending: discovering desistance' (Institute for Research and Innovation in Social Services, University of Glasgow 2012) 3
[131] M. Farmer, A.M McAlinden and S. Maruna, 'Understanding desistance from sexual offending: A thematic review of research findings' (2015) 62(4) Probation Journal 320, 322
[132] M. DeLisi, 'Age-Crime Curve and Career Criminal Patterns', cited in J. Morizot and L. Kazemian, *The Development of Criminal and Anti-Social Behaviour, Theory, Research and Practical Applications* (Springer Publishing 2015) 52
[133] D. P. Farrington, B. Gallagher, L. Morley, D.J. West and R.J. St Ledger, 'Cambridge Study in Delinquent Development; Long-Term Follow-Up' (Unpublished manuscript. Institute of Criminology, Cambridge University, 1988)
[134] Above n.120, 3

behaviour peaks in their teenage years, and then starts to decline',[135] while Delisi is yet more blunt:

The association between age and criminal offending is a brute fact. It does not require explanation because it is a constant seen in offending data across nations, across historical periods, across data sources, across sample composition and across forms of problem behaviour.[136]

For some offenders, desistance comes after a brief pattern of offending[137] which usually lasts not more than five years,[138] after which time no further convictions are obtained. Offenders who reach age thirty and are still committing offences are generally rare, and such individuals will usually only desist after a 'career' of ten years, where they desist at all.[139] Individuals who commit their first offence after age thirty are rare. One study into these found that they usually have short criminal 'careers' lasting less than three years in total, with recidivism rates of 42.1% and commit less than two offences each on average.[140] By age forty, almost all offenders desist and rates of new convictions for those aged forty or over are very low indeed; one official study found that of the population of England and Wales born in 1953, only 3% were convicted of a first offence after reaching aged 38.[141]

For a majority of those convicted of an offence, desistance occurs very quickly indeed and it is the case that 'most offenders only have one court appearance resulting in a conviction'.[142] Even among juvenile offenders, single-conviction records have a high prevalence; one Ministry of Justice longitudinal study in 2001 found that 44% of juveniles convicted of a first offence in 2000 had no further convictions when their records were re-examined in 2009.[143] Indeed, a further Ministry of Justice study of all aged, known offenders and offending rates showed that, among members of the population born in 1953, 33.2% had a criminal record containing at least one conviction.

[135] Above n.129
[136] Above n.131, 51
[137] Above n.114, 11 – 22
[138] J. H . Laub and R. J. Sampson, 'Understanding Desistance from Crime' (2001) 28 Crime and Justice 1 – 69, 17
[139] Ibid
[140] Above n.125, 536
[141] Ministry of Justice, 'Conviction histories of Offenders between the ages of 10 and 52. England and Wales' (15 July 2010) 4
[142] Above n.139, 7
[143] Above n.128

Of that proportion of individuals, 51.8% had only one conviction. Of the remainder, most offenders desisted relatively quickly; 16.6% of those with a criminal record had two convictions while only 18.1% had five or more convictions.[144] Analysis of subsequent cohorts of individuals born in five-year intervals from 1953 to 1973 showed an almost identical pattern, with around 50% of those with convictions by age thirty having only one conviction.[145]

What emerges, then, is that juveniles are more disposed to criminality than adults, that juveniles and young adults are more likely to be convicted of offences than adults, that criminality tends to tail off at around the mid-twenties or early thirties (at the latest) and that although reconviction rates are high, there are significant proportions of those convicted of offences who are either not reconvicted at all or are reconvicted of only one or two further offences. Only a very small, but nonetheless significant, proportion of those who are convicted of an offence go on to commit significant numbers of further offences.

It follows, then, that PHOENIX must contain a significant number of records, likely in the millions, of individuals who have committed either one single offence or who have committed a small number of offences and have since been of no interest to the police whatsoever. Very many records, again likely numbering in the millions, will likely show a 'cluster' of offences committed by individuals in their youth who have since desisted from offences and not come to the attention of the police since. The records much more likely to have operational value to the police are those of recidivistic offenders who have not yet desisted. These are statistically significant, but a minority of the total holdings nonetheless; perhaps one-fifth of the PHOENIX holdings will relate to such individuals, but not much more than this.

The key additional variable here is time since last conviction; the so-called 'clear period'. Most of the studies undertaken use a 'follow-up' period of between six months and two years because to properly measure reconviction rates over a lengthy period requires a difficult and necessarily longitudinal study, but it is nonetheless widely accepted, even by keen proponents of 'propensity' as an evidential tool, that the longer a person goes without reconviction, the less likely they are to commit a further offence.

[144] Ibid 8
[145] Ibid

Convictions are likely to have probative value where they are 'recent'; although a convicted person will remain statistically more likely to commit another offence than an unconvicted person for the remainder of their life, the relative likelihood will decrease steadily over time.[146]

In 2012 the Ministry of Justice conducted a comprehensive analysis of recidivism rates over a nine year period following proven re-offending rates among the 617,024 or so individuals convicted, cautioned, reprimanded or warned in 2000.[147] All of the data was taken from the PNC.[148] It found similar patterns to those found in the shorter studies; namely that re-offending rates were higher among juveniles than among adult offenders,[149] that those who committed four or more offences committed the most re-offences (56% of the total) and that a small number of prolific recidivists (the most prolific 1% of re-offenders) committed 7% of re-offences.[150]

What the study also showed, though, was that re-offending rates continued to increase beyond the ordinary two-year follow-up period. By the end of two year, the overall re-offending rate for all offenders was 38.9%. After a further year, this increased to 45.6%, and to 50.2% after a fourth year. Interestingly, although re-offending rates continued to increase throughout the nine-year study, these began at five years to flatten quite markedly, with subsequent increases of 2%, 2%, 1.5%, 1.2% and 1% up to 58.9% overall after nine years.[151]

While this certainly shows that re-offending rates over time are higher than those indicated in the shorter follow-up studies, what is also shown, it is submitted, is that after five years the rate of increase is very markedly smaller, and following a consistent downward trend. It must be presumed, therefore, that subsequent years would show a similar reduction in re-offending rates, until eventually the increase either stops or becomes sufficiently negligible as to be statistically insignificant.

What is also significant, it is further submitted, is that even after nine years, the number of individuals who are not re-convicted of further offences remains very high. In short,

[146] Above n.97, 696 – 7
[147] Ministry of Justice, '2012 Compendium of re-offending statistics and analysis' (12 July 2012)
[148] Ibid, 12
[149] Ibid, 32
[150] Ibid at 44
[151] Ibid at 37

41.1% of all those convicted in 2000 had committed no further offences in the nine-years subsequent. Presuming that the studies highlighted early are correct, this should mean that these individuals (or at least a very large proportion of them) had desisted, and would thereafter be of very little value to police in either crime prevention or crime detection.

The 2012 study also provided an interesting analysis of re-conviction rates as compared to the original 2000 disposal. These show that re-conviction rates among those disposed of by caution showed a similar pattern to the general re-conviction trend, so that well over half of those re-convicted were so disposed in the first two years, and that by five years the vast majority of those who were reconvicted at all had been so, but also that re-conviction rates were much lower than the overall rate; 23.3% after two years, 34.7% after five years and 38% after nine.[152] Although they too followed the same pattern of diminishing likelihood over time, re-conviction rates for those handed a custodial sentence were much higher; 59.4% at two years, 72.5% at five years and 78.4% at nine.[153]

This seems to support a dual contention. The first is that those who commit less serious offences (and are subsequently cautioned) are far less likely to be reconvicted of a subsequent offence than those who commit more serious offences (and are subsequently given a custodial sentence). This might support the position taken in Scotland, where 'serious' offences are retained under the '70/30 rule', rather than the '40/20 rule'. That notwithstanding, even the most serious offenders often desist; one recent study in Canada found that even those convicted of sex offences will often desist to almost the same level of non-reconviction risk as non-offenders, albeit at roughly double the 'clear-period' as those convicted of non-sex offences.[154]

It is submitted that there exists a significant body of academic literature to show that desistance is sufficiently evidenced that there must exists a significant question mark over police claims that the retention of records on PHOENIX until each data subject reaches age 100 years aids in police operational processes. What this literature shows is that, while a criminal disposal does increase the likelihood of re-conviction, and that

[152] Ibid, 41
[153] Ibid
[154] Above n.91, 1342 – 43

this might allow police to focus resources on 'known' offenders, this likelihood decreases significantly over time even among those who do actually commit further offences or among those who commit serious offences.

It therefore follows that there are many individuals, likely numbering in the millions, who are subject to PHOENIX listings which are now entirely inactive because the individuals listed either are not committing offences or are not being suspected of offences or in any event being reconvicted of them. There exists, therefore, a strong argument in favour of deleting at least some of these nominal listings from PHOENIX once a suitably lengthy 'clear-period' has passed to show that the individual has desisted.

It is precisely this argument that was made by Soothill and Francis during the *Five Constables* case, and, it is submitted, the Court of Appeal were in error in treating it so dismissively. If the police contend that this position is in error, and minor and entirely inactive PHOENIX listings really are of 'operational value', then surely it is for them to make their case far more persuasively than the various anecdotal attempts that have been made to date. It should not be hard for them to do so; as the data controllers for the PHOENOX data they are uniquely placed to use their own data to show the value of their repository of criminality data. That they have failed entirely to do so, despite numerous opportunities afforded to them, must indicate that they are unable to show this, and their continued reliance on Parliamentary and judicial deference to them on their 'operational needs' further strengthens this contention.

It is submitted that there remains no empirical support for the position offered by chief officers in England that the PHOENIX collection meaningfully assists in preventing and detecting crime. In truth, it is further submitted, the position is that described by Lord Kerr (albeit in reference to biometric criminality data):

It is difficult to avoid the conclusion that the fact of conviction merely provides the pretext for the assembly and preservation of a database which the police consider *might* be useful at some time in the future and that it has no direct causal connection to the actual detection of crime and the prevention of future offending.[155]

[155] Above n.35

8.5 The deletion of certain records would solve the disclosure problem

The problems inherent in the police retention police for criminality data have, over the last fifteen years, manifested themselves most abundantly when the PHOENIX data is used to perform a criminal record check on an individual subject to a nominal listing. There is a general, and it is submitted, mistaken, view that the retention of criminality data, and the subsequent use of it for criminal vetting purposes, are analogous. This error was made by Waller LJ in *Five Constables* case, who claimed that:

> It is important to emphasise at the outset that the complaint about retention flows in reality not from the retention itself but from the fact that, if retained, disclosure may follow.

For reasons that will be made explicit in the next chapter of this research, such a simplistic approach is manifestly incorrect, because the (arguably unlawful and/or disproportionate) retention of data is a ground for legal challenge. Data Protection legislation affords legal rights and obligations in respect of unlawful data processing *per se*, where 'processing' includes collection, recording and storage.[156] That disclosure follows from it is merely incidental, or perhaps better described as a different form of processing, to which near identical data protections apply[157] and which ought additionally be borne in mind when determining the lawfulness of the retention itself.

This is why this research has intentionally refrained, to as large an extent as possible, to refer to the disclosure of PHOENIX data in criminal record checks. The purpose of this research has been to highlight data protection deficiencies in the PHOENIX collection itself, rather than its use for vetting purposes, which, unlike the data retention deficiencies highlight in this research, has now began to attract extensive academic, judicial and legislative attention. However, it would be remiss not to at least address one particular issue in criminal record disclosure which could be rectified almost immediately if the recommendations of this research were to be implemented, even in part.

This author has already outlined elsewhere the extensive, historical use of police collections of criminality data for vetting individuals applying for employment and voluntary

[156] Per s.3(4)(a) of the Data Protection Act 2018
[157] Ibid, s.3(4)(d)

positions, as well as for visa applications and other safeguarding concerns.[158] This was despite a police and Home Office supposition that the collection of criminal records was not to be used for vetting purposes unless exceptional circumstances justified otherwise.[159]

This position was bulwarked by statute. In 1972, an independent committee, set up by NACRO, the Howard League for Penal Reform and the Ministry of Justice and headed by Lord Gardiner, published a report[160] which provided that 'most civilised countries recognise that it is in their interest to accept back into the community a person who, despite one or more convictions, goes straight for a sufficient number of years'.[161] At the time the UK was the only western European country who did not limit the disclosure of criminal records in any way.[162] Gardiner's recommendation was that where a person has shown by their conduct subsequent to their conviction for an offence that they have rehabilitated themselves, the law should (subsequent to limited exceptions) treat that person as rehabilitated and 'restore the offender to a position in society no less favourable than that of one who has not offended'.[163]

The result was the Rehabilitation of Offenders Act 1974 (the 'ROA 1974'), intended 'to support the rehabilitation into employment of reformed offenders who have stayed on the right side of the law'.[164] The ROA 1974 does this by allowing a convicted person to consider that a conviction is 'spent', and therefore does not have to be disclosed when asked to disclose a criminal record,[165] so long as they were not reconvicted of a new offence during the designated clear period.[166]

This relatively simple premise has, in practice, become a set of incredibly complex provisions, due in part to the differing rules which try to balance the severity of the original offence and the qualifying period which should be attached. The original provisions have

[158] C. Baldwin, 'The Vetting Epidemic in England and Wales' (2017) 81 Journal of Criminal Law 478
[159] Home Office, 'Police reports of convictions and related information (HOC 140/1973)
[160] The Gardiner Committee, *Living it Down – the problem of old convictions* (London, Stevens and Sons 1972)
[161] Cited in 'Discussion Paper on the Rehabilitation of Offenders Act 1974' (The Scottish Government, 27 August 2013) 6
[162] Ibid.
[163] Above n.161, 7
[164] Ministry of Justice, 'Guidance on the Rehabilitation of Offenders Act 1974' (4 March 2014) 3.
[165] S.4(3) of the Rehabilitation of Offenders Act 1974
[166] S.1(1) of the Rehabilitation of Offenders Act 1974

been repeatedly amended,[167] with the most recent coming in March 2014 when Chapter 8 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012 came into force. This provides that a conviction which results in a custodial sentence of forty-eight months is automatically never spent.[168] Reductive changes to almost all other rehabilitation periods were made, so that convictions resulting in custodial sentences of between thirty and forty-eight months are spent seven years after the day that the relevant sentence is completed. The rehabilitation period for offenders sentenced to between six months and thirty months was reduced to four years and the period where the sentence imposed was less than six months was reduced to two years. The period of rehabilitation where an offender was fined was reduced to one year.[169] Cautions are spent as soon as they are issued.[170]

The ROA 1974, however, has never been universally applicable. Shortly after the creation of the ROA 1974, the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975[171] ('the 1975 Order') was enacted[172]. This provides exemptions from the spent conviction rules because 'while it is generally desirable to effect the rehabilitation of offenders and help them into employment, the public must be adequately protected in certain respects'.[173] These occur, broadly speaking, when someone applies to a post involving contact with children[174], vulnerable adults[175] or large sums of money[176] or when a question is asked relating to any of the professions listed in Schedule 1 of the 1975 Order (which includes teachers, solicitors/barristers and many other professional positions). As Carnwath LJ said in the *Five Constables* case: 'there are many (arguably too many) exceptions to the principle of spent convictions.[177] The excretions into the spent conviction principle seem to perpetuate routinely – some of those now included are stewards at

[167] The Criminal Justice Act 1982, Criminal Justice Act 2003, Armed Forces Act 2006 are but three pieces of legislation to add to or amend the ROA 1974.
[168] Per s.139(2) Legal Aid, Sentencing and Punishment of Offenders Act 2012
[169] Per s.139(4) Legal Aid, Sentencing and Punishment of Offenders Act 2012
[170] Per s.65(9) Crime and Disorder Act 1988
[171] SI 1975/1023
[172] As authorised by s.4(4) of the Rehabilitation of Offenders Act 1974
[173] *R (on the application of W)* v The Secretary of State for justice [2015] RWHC Admin 1952 [10]
[174] Art. 3(1)(a) of the Rehabilitation of Offenders Act (Exceptions) Order 1975
[175] Art 3(1)(aa) of the Rehabilitation of Offenders Act (Exceptions) Order 1975
[176] Art 3(1)(e) of the Rehabilitation of Offenders Act (Exceptions) Order 1975
[177] Above n.1 [77]

football matches, members of the Master Locksmiths Association,[178] traffic wardens, taxi drivers and vets.[179]

Until 1992, all answers to 'exempted questions' could be obtained by asking the police to check their records and return a 'police report of character' on the individual in question. The police bore the cost of these and issued them almost entirely at their discretion.[180] Where the police refused, or where the employer wanted to ask a question which was not 'exempted', many individuals were told to make subject access requests[181] to obtain copies of their police record prior to employment. These 'DIY checks' were only outlawed in March 2015.[182] Such unlawful checks are not uncommon: one investigation found that some 11% of checks requested in 2005 were illegal (i.e. they did not relate to an exempted question)[183]

In September 1993, the Government issued a consultation document[184] proposing to put criminal record disclosure on a statutory footing.[185] Largely resultant of police complaints that they were wasting valuable time and resource conducting checks and simultaneous pressure from employers and voluntary groups who wanted increased access to police records,[186] the consultation proposed opening up criminal record checks to largely anyone who wanted them[187] and commodifying them; allowing them to be 'sold' by a new organisation independent of the police.[188]

The Government initially hesitated for fear of a public backlash, but the reaction instead was one of 'complete indifference'.[189] Duly emboldened, the Government then moved to pass the Police Act 1997,[190] which created the statutory framework for criminal record

[178] Above n.174
[179] 'Growing up, moving on. A report on the childhood criminal records system in England and Wales' (Standing Committee on Youth Justice, June 2017) 6
[180] Home Office, 'Disclosure of Criminal Records for Employment Vetting Purposes' (Cm. 2319, 1993) 11
[181] Per s.21 DPA 1984 or s.7 DPA 1998
[182] Per s.56 DPA 1998 as amended by The Data Protection Act 1998 (Commencement No. 4) Order 2015
[183] R. Suff, 'Checking out the activities of the Criminal Records Bureau', (2005) 483 *IRS Employment Review* 42–48
[184] Above n.180
[185] Ibid, 20
[186] T. Thomas, "Employment Screening and the Criminal Records Bureau' (2002) 31(1) Industrial Law Journal 55, 61
[187] Above n.184, 13
[188] Ibid, 19
[189] Above n.158, 485
[190] ch.50, 1997

disclosure. The regime, which has been amended so often since that the Law Commission described it in 2017 as 'hard to understand and inaccessible to users',[191] broadly provides for three different types of criminal record disclosures. The first is the 'basic check', which provides all unspent convictions and conditional cautions[192] held in 'central records'.[193] These can be obtained by any employer in any circumstance.[194] A 'standard check' provides details of 'all relevant matters' held on police records.[195] As originally enacted, a standard check was intended to answer exempted questions,[196] therefore 'all relevant matters' were all convictions, cautions, reprimands and warnings, spent or unspent, kept in 'central records'.[197] It is perhaps worth noting that there is nothing in the legislation which provides that 'central records' are themselves a 'complete record' and certainly they were not supposed to be so in 1997 when the Police Act came onto the statute book; the police were (allegedly) weeding records at that time with Home Office complicity and occasional Parliamentary debate on that subject.

The most stringent check is the 'enhanced check'. As originally prescribed, these were intended only for those with regular contact with children,[198] vulnerable adults[199] or one of many specified positions listed in the statute or in other legislation.[200] These also included all convictions and cautions, spent or unspent,[201] as well as information provided by a chief officer, which in the chief officer's opinion, 'might be relevant' and 'ought be included'.[202] The 'information' included as a chief officer's discretion was to later found to be largely taken from both the PNC 'event history' and the Police National Database, such

[191] The Law Commission, *Criminal Records Disclosure: Non-Filterable Offences* (Law Com. No.371, 31 January 2017) 9
[192] Per s.112(2)(a) of the Police Act 1997, as amended by s.84(a) of the Protection of Freedoms Act 2012. Simple cautions are therefore not disclosed on a basic certificate, nor are spent convictions.
[193] Defined by s.112(3) of the Police Act 1997 as 'such records held for the use of police forces generally'.
[194] 'DBS checks: guidance for employers' (*Disclosure and Barring Service,* 3 April 2019.<https://www.gov.uk/guidance/dbs-check-requests-guidance-for-employers#overview> (accessed 16 April 2019)
[195] Per s.113(3)(a) of the Police Act 1997
[196] Per s.113(2) of the Police Act 1997
[197] Per s.113(5)(I)(ii) of the Police Act 1997
[198] Per s.115(3) of the Police Act 1997
[199] Per s.115(4) of the Police Act 1997
[200] Per s.115(2)(b) of the Police Act 1997
[201] Per s.115(6)(a)(i) of the Police Act 1997
[202] Per s.115(7)(a)(b) of the Police Act 1997

as allegations made which resulted in no charge,[203] acquittals,[204] criminal contacts with family members[205] and contact with social services.[206]

The entire system of disclosure was to be administered by an independent, public/private body who would have 'read-only' access to PHOENIX for the purpose of conducting checks and issuing disclosure certificates.[207] The Criminal Records Bureau ('the CRB') was opened in March 2002[208] and was immediately deluged by disclosure applications in the wake of the *Soham* murders.[209] The subsequent opening of the vetting floodgates led to what this author has described elsewhere as 'a vetting epidemic in England and Wales',[210] with criminal record disclosures rising from around 900,000[211] in 1992, 1.76 million in 2002[212] to 3.3 million in 2007.[213]

The CRB was plagued by controversy from its inception and was closed December 2012 and replaced by the Disclosure and Barring Service ('the DBS') in December 2012.[214] The DBS has continued the commercialisation and expansion of criminal record disclosure started by its predecessor; it's most recent annual accounts proudly boasting of adding the issuing of basic checks (which were only finally 'launched' in January 2018) to its 'existing Disclosure products'. Last year it issued a total of 4.6 million criminal disclosure checks.[215]

---

[203] *R (on the Application of John Pinnington) v Chief Constables of Thames Valley Police* [2008] EWHC 1870 (Admin)
[204] *R (on the application of S) v Chief Constable for West Mercia Constabulary* [2008] EWHC 2811 (Admin)
[205] *R (on the application of SL) v Chief Constable of the Metropolis* [2008] EWHC 1442 (Admin)
[206] *R on the application of L) (FC) (Appellant) v Commissioner of Police of the Metropolis (Respondent)* [2009] UKSC 3
[207] The Disclosure and Barring Service is one of forty-two non-police agencies with such access, as indicated by a response to a Freedom of Information request made in the course of this research; see Home Office, 'FOI Request. Request for information regarding access to the Police National Computer' (FOI Case Ref: 49917 *What do they Know?* 21 August 2018) <https://www.whatdotheyknow.com/request/request_for_information_regardin_120#incoming-1236064> accessed 21 August 2018
[208] Above n.158, 491
[209] Above n.6
[210] Above n.158
[211] Ibid, 483
[212] Ibid, 491 – 92
[213] Ibid, 493
[214] Above n.6
[215] Disclosure and Barring Service, 'Annual Reports and Accounts for the period 1 April 2017 to 31 March 2018' (HC 1367, 19 July 2018) 8

Those subjected to disclosures which cost them employment opportunities were understandably less impressed by the CRB/BDS's 'product', and very quickly the police found themselves facing legal challenges to the disclosure of records under the Police Act 1997. These have followed two broad lines. The first involve challenges to the 'additional information' included on enhanced certificates.[216] These saw a reconfiguration of the test to be used when deciding whether such disclosure is Human Rights compliant,[217] recommendations to reformulate the statutory framework[218] and ultimately primary legislation to have resulted in amendments to the legislative framework[219] which made the test for disclosure more stringent[220] and introduced an independent monitor[221] to oversee disputes over intelligence data use.

This line of criminality data dispute largely lies outwith the scope of this research, save a passing interest in the possible use of 'event histories' as part of disclosures.[222] The second line of challenge, which has far more relevance to this research, involves the disclosure of old and minor convictions as part of 'standard' criminal record checks. As we have seen, until 2006 the police were in the habit of deleting old and minor criminal records (or at least they had a policy which stated that they were supposed to do so). This, presumably, must have been in the knowledge of Parliament when they passed the 1997; as has been shown, 'weeding policies; had been discussed by Government ministers and backbenchers alike in Parliament for many years prior to the passing of the Police Bill in 1996. It must reasonably be presumed, therefore, that Parliament intended for the new criminal record regime to disclose the criminality data available on the PNC, rather than any complete record.

That notwithstanding, once the police abandoned their weeding policy, endorsed by the decision in the *Five Constables* case, judicial review challenges, based on a lack of

[216] A detailed exposition of the lineage of these, along with critical analysis of several key judgments including the leading decision in *R (on the application of L)* (above n.206) was produced by the author in C. Baldwin, 'Necessary intrusion or criminalising the innocent? An exploration of modern criminal vetting' (2012) 76(2) Journal of Criminal Law 140 – 163
[217] Above n.206 [42]
[218] S, Mason, 'A Balanced Approach' (Home Office, March 2010) 26 – 27
[219] Per the Protection of Freedoms Act 2012, ch.9
[220] Per s.82(1 – 4) of the Protection of Freedoms Act 2012, inserting new provisions into s.113B of the Police Act 1997. Section 113B is now the provisions which deals with enhanced criminal record checks after s.115 of the Police Act was repealed by Sch.17, Pt.2 of the Serious Organised Crime and Police Act 2005, ch.15
[221] Per s.82(5) of the Protection of Freedoms Act 2012, inserting s.117A into the Police Act 1997. The Independent Monitor was created by s.119B of the Police Act 1995.
[222] For a fuller examination of the position regarding enhanced disclosures, see above n.216

proportionality as balanced against human rights concerns,[223] began to emerge against the disclosure of minor or aged criminality data on standard certificates.

In R (on the application of T and another) v Secretary of State for the Home Dept. and another,[224] an individual who had been given two police warnings for bicycle thefts as juvenile and another who had been given a police caution for the shop-theft of a packet of false fingernails contested the inclusion of these on a standard criminal record check which had resulted in their removal from a university course and employment as a care sector worker respectively.[225] The Supreme Court held that the disclosure of this information was 'not in accordance with the law' because the blanket nature of the statutory regime meant that there were no safeguards against the kind of arbitrary interference in rights which occurred in these cases.[226] It also found that such disclosure was not 'necessary in a democratic society', because these disposals bore 'no rational relationship to the aim of protecting the safety of children' or ''was disproportionate to the likely benefit in achieving the aim of protecting people receiving care'.[227]

What no-one, including the Government, seems to have recognised is that these warnings and cautions would have been deleted until the 2002 Weeding Rules, had these remained in force, and so would not have been available for disclosure. Had the Government recognised this, it might have found a ready answer to the problem the Supreme Court had set for it.

Instead, the Government decided to try and implement a statutory 'filter'[228] to allow the police to retain all of the PHOENIX data but to disallow the inclusion of certain aged, minor criminality data on standard disclosure certificates. These created 'protected cautions',[229] which are those cautions which do not relate to a 'listed offence' and were issued two or more years ago (for juveniles)[230] or six or more years ago (for adults).[231] These were not

[223] A full examination of the Article 8 ECoHR position is offered in the next chapter of this research.
[224] [2014] UKSC 35
[225] Ibid [4][5]
[226] Ibid [119]
[227] [121]
[228] The Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (Amendment) (England and Wales) Order 2013/1198
[229] Ibid, s.3(2)
[230] Ibid, s.4(1)(a), inserting Article 2A into the 1975 Order
[231] Ibid, s.4(1)(b), inserting Article 2A into the 1975 Order.

be to disclosed.[232] A protected conviction[233] is one which does not relate to a 'listed offence',[234] which did not result in imprisonment or a detention order[235] and which was disposed five and half (for juveniles)[236] or eleven years (for adults) previously.[237] These would not be disclosed as long as no other convictions or cautions were recorded.[238] 'Listed offences' included almost all serious sexual and violence offences and a wide array of other 'non-filterable offences'.[239] The list is very inaccessible, according to the Law Commission, as it is variously contained in different statutes and in an 'operational list' maintained by the Home Office.[240] The list is very substantive, and seems to expand exponentially; this author submits that there are, at April 2019, some 1,000 or so 'listed offences' offences which are never filtered.

What is of interest to this research is that what the Government had effectively attempted to do was to implement a statutory 'step-down' process, similar in nature to, but wildly more restrictive than, the step-down process initiated by ACPO in 2006 and abandoned after the *Five Constables* case. Remarkably, and almost by accident, the decision in *R(T)* and the Government response to it has effectively overturned the decision in the *Five Constables* case, or at least that portion of it which relates to the step-down process.

However, it was immediately apparent that the new 'filter' would be challenged; one analysis described the filter as 'slightly more nuanced but still very restrictive and does not reflect an adequate balance…two minor offences will always be disclosed'.[241] In Gallagher's Application for Judicial Review,[242] that concern was deemed sufficient to declare that the filtering system was still unlawful, but this time on the limited grounds that a 'multiple conviction rule' does not properly reflect the severity of offences or propensity to offend and may produce 'eccentric consequences' which are disproportionate.[243] The

[232] Ibid, s.5, amending Article 3 of the 1975 Order.
[233] Above n.229
[234] Above n.228 s.4(3)(a), inserting Article 2A into the 1975 Order.
[235] Ibid, s.4(3)(b) and s.4(4), inserting Article 2A into the 1975 Order.
[236] Ibid, s.4(2)(a), inserting Article 2A into the 1975 Order.
[237] Ibid, s.4(2)(b), inserting Article 2A into the 1975 Order
[238] Ibid, s.4(3)(c), inserting Article 2A into the 1975 Order.
[239] Ibid, s.4(5)
[240] For a summary of this, and the problems pertaining to the list, including errors, inaccuracies and the sheer difficulty for lawyers and non-lawyers in trying to find the relevant information, see above n.191, 37 – 79
[241] E. L. Pijoan, 'Criminal record disclosure and the right to privacy' (2014) 10 Criminal Law Review 723 – 737, 734
[242] [2019] UKSC 3
[243] Ibid [63]

majority of the Supreme Court also found that the potential disclosure of reprimands, warnings and youth cautions was a 'category error' and 'an error in principle' because the disclosure of these was in direct contravention of the rehabilitative and redemptive purpose of these disposals.[244]

The net result is that the Government will once more have to revisit their 'filter'. Early indications are that they intend to add more 'filters', so that less disposals, especially those involving juveniles, will be disclosed.[245] The merits or otherwise of such an approach are for a different research piece to this, but it is submitted that the Government might want to consider a simple point of principle elucidated by the European Court of Human Rights which might offer a far less complex solution to the problem it has created:

> It is clear that if the applicant was able to have her data deleted, then it would no longer be capable of disclosure.[246]

8.6 Conclusions

The decision in the *Five Constables* case is open to criticism in many regards. It misrepresents the use of criminality data in the criminal justice system; a disingenuous position offered by the very individuals who ought to know the true position. It further makes the common error of relying on *Soham* as justification for iniquitous practices which disproportionately impact on the rights of citizens not to be subject to excessive data collation. This error is perhaps understandable among news-media and internet writers. It is fundamentally obtuse when made by appellate judges.

The most damaging error, however, is in deferring entirely to the word of police officers on the 'usefulness' of criminality data which does not stand to scrutiny when placed against the countless academic studies which show that old, inactive criminal records offer little assistance in either the prevention of new offences or the detection of these. If the police, who in PHOENIX hold the single largest repository of criminality data in England and Wales, continue to claim that this data is of operational use, the onus must now be on them to offer empirical support for that proposition, particularly in light of the widely

[244] Ibid [64]
[245] C. Hymas, 'Criminals to be handed clean slate under Sajid Javid plan to wipe minor offences when applying for jobs' *The Telegraph* (London, 16 April 2019)
[246] *MM v the United Kingdom* [2012] ECHR 24029/07 [159]

accepted consensus positions that most offenders, even the most serious ones, desist from their offending behaviour after a sufficiently lengthy passage of time.

The police posit that an isolated conviction for theft recorded a decade or more previously is of operational value to them. This position is contrary to both academic research and common sense. It cannot continue to be left unchallenged by the very organs of the state whose role is to afford members of the public an opportunity to put police processes under scrutiny.

For decades, the police accepted that deleting certain records was of no operational impact to them. That position remains extant in Scotland, where presumably police have the same operational values and processes but where records continue to be deleted once a sufficient passage of time indicates that these are of sufficient irrelevance that their continued retention is excessive, for data protection (and indeed any conceivable) purposes. There are no suggestions that deletion there impinges upon the prevention or detection of offences, the processes of the criminal justice system or that these raise the spectre of child abduction offences.

The risk of deleting such records, based on the experience of Scottish criminal justice and scores of criminological studies, is extremely small. The continued retention of that data conflicts with data protection principles and is causing significant problems with the disclosure of criminality data, which both could be simply avoided if a deletion process, properly considered and empirically based, was reinstated.

9
The scope for a European jurisprudential challenge to the *Five Constables decision*

9.1 Introduction

If the decision in the *Five Constables* case cannot be successfully revisited on the grounds outlined in the previous chapter, it may in the alternative (or perhaps even concurrently) be possible to do so by an alternative means linked to, but not strictly limited by, the applicable Data Protection legislative provisions.

In this final substantive chapter of this research, which concludes the substantive analysis and evaluation of the fourth research question, the author will return to themes identified and analysed in Chapter 2 and consider whether the indefinite retention of criminality data by the state on PHOENIX might contravene human rights provisions. This will be done by examining the legislation and jurisprudential developments in respect of the police national collections of DNA and fingerprints ('Biometric Criminality Data' or 'BCD') and custody images – the historical and contemporary bedfellows of the collection of criminality data held on PHOENIX – which have transpired since the *Five* Constables case and analysing how the principles posited in these might reasonably be transferred to the PHOENIX data collection in future.

9.2 The 'Right to Privacy'

The European Convention on Human Rights and Fundamental Freedoms 1950 ('the ECoHR') provides a number of fundamental rights and freedoms applicable to citizens of each state (which includes the United Kingdom) which is a signatory. Of particular relevance is Article 8(1) of the ECoHR, which provides that:

> Everyone has the right to respect for his private and family life, his home and his correspondence.

This is a qualified right, as per Article 8(2) it is provided that:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic

society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8(1) is usually expressed as providing a qualified 'right to privacy'. It had long been presumed that criminality data, particularly that collected on PHOENIX, did not 'engage' Article 8(1) because convictions occur in court, which is open to the public and press, so that a conviction (and data relating to it) could not constitute 'private' data[1] and so any challenge relating to the lawfulness of the data must fail. '

9.3 Criminality data and Art.8: the decision in *MM*

In the *Five Constables* case, the Information Commissioner made detailed representations that the retention of criminality data engaged Article 8(1). These were dismissively rejected in two paragraphs of the judgment. Firstly, Waller LJ simply stated that 'I am not persuaded that Article 8(1) is engaged at all in relation to the retention (original emphasis) of the record of a conviction…Even if that were wrong, the processing is in accordance with the law and necessary in a democratic society'.[2] The judge rather unhelpfully offered no further explanation as to why either of these views were expressed.

Carnwath LJ agreed,[3] positing that the public nature of court proceedings meant the fact of conviction must be public information, before dismissing any analogy to the almost simultaneous litigation[4] brought regarding the indefinite retention of all DNA samples by police, because he believed that a distinction should be drawn between data held on those whose guilt had not been formally determined and those with convictions whose guilt had so been.[5]

While certainly more balanced than the position offered by Waller LJ, this analysis rather ignores the matter of cautions, which are not legally considered 'convictions' (although they do involve an admission of guilt on the part of the recipient), warnings and reprimands (which require no admission of guilt at all) and PNfDs (which imply no finding of guilt

[1] [2009] UKSC 3 [27] (Lord Hope)
[2] [2009] EWCA Civ 1079 [50] (Waller LJ)
[3] Ibid [79] (Carnwath LJ): 'there is considerable doubt in any event whether recording the mere fact of a conviction can ever engage article 8 of the ECoHR…the bare fact of conviction should not be regarded as private information'
[4] *S and Marper v UK* [2008] ECHR 30562/04
[5] Above n.2 [79] [80]

whatsoever) – all of which are held in the PHOENIX repository and which are not formally issued in the public forum of the courtroom. Indeed, as has been shown, one of the predominant advantages to the recipient of these disposals is that they are usually issued in private. It should be recalled, perhaps, that one of the five individuals in the *Five Constables* case was seeking the deletion of a reprimand, rather than a conviction, which makes this oversight rather more surprising.

The notion that Article 8 was not engaged by the mere retention of criminality data was fatally undermined a matter of days after the *Five Constables* decision, when the Supreme Court passed its judgment in *R (on the Application of L) v Metropolitan Police Commissioner*.[6] Although this case involved the retention and disclosure in a CRB criminal record check of non-conviction data, Lord Hope fully addressed the issue of conviction retention:

> Information about an applicant's convictions which is collated and stored in central records can fall within the scope of 'private life' within the meaning of Article 8(1). It is, in one sense, public, because the convictions took place in public. But the systematic storing of this information in central records means that it is available…long after the event when everyone other than the person concerned is likely to have forgotten about it. As it recedes into the past, it becomes part of the person's private life which must be respected. Moreover [many of the disposals recorded] …takes place behind closed doors. A caution takes place in private [or] it may include allegations of criminal behaviour where there was insufficient evidence to prosecute.[7]

The notion that the collation and retention of criminality does not engage Article 8(1) was definitively shown to be misconceived by the European Court of Human Rights ('the ECtHR') in *MM v the United Kingdom*.[8] The facts in *MM* bear a rather striking similarity to those in the *Five Constables* case. MM had made an ill-advised attempt to help reconcile the separation of her son and daughter in law, the latter having intimated that she was to leave Northern Ireland and return to Australia with the applicant's grandchild, by taking her granddaughter and not returning the child to her mother at an appointed time.[9] The

[6] Above n.1
[7] Ibid
[8] [2012] ECHR 24029/07
[9] Ibid [6]

police were called and the child was found, unharmed and with the applicant, and returned to her mother the next morning. The decision was taken not to charge MM but instead to issue a caution for 'child abduction',[10] which was duly recorded on 'Causeway'; the Northern Irish equivalent to PHOENIX.[11]

In response to a query raised by MM three years later, the police confirmed that the caution would be retained for a total of five years in accordance with the 2000 Weeding Rules.[12] However, that caution was not deleted because the police in Northern Ireland appeared to have taken lead from, and followed, the 2006 Guidelines so that nothing was 'weeded' from the system at all after these were implemented.[13] MM became aware of this when she subsequently applied for a position as a family support worker. Her criminal record check revealed the caution and her application was refused, notwithstanding an additional clarification provided by the Northern Ireland Criminal Records Office explaining the circumstances of the caution.[14]

She duly complained to the Criminal Record Office and the police data controller, both of whom sympathised and offered to provide additional information to assist for vetting purposes, but both refused to delete the caution.[15] When she applied, and was rejected after a criminal record check, for a second similar employment post, she issued proceedings directly to the ECtHR to have the caution deleted from her record.[16]

The Government initially represented that MM should have her case struck out as an abuse of process, arguing that she should have first either complained to the Information Commissioner, issued judicial review proceedings against the police, or both.[17] This argument was dismissed for reasons abundantly apparent from the analysis provided in chapter seven of this research; any judicial review proceedings, brought at considerable cost and time, would inevitably fail under the applicability of the precedent set in the *Five Constables* case, while an application to the Information Commissioner would have amounted to little more than a fruitless paper-chasing exercise for much the same

[10] Ibid [8]
[11] Ibid [37]
[12] Ibid [10]
[13] Ibid [13]
[14] Ibid [11 – 12]
[15] Ibid [13] [16]
[16] Ibid [19]
[17] Ibid [154]

reasons.[18] The Court then moved to consider whether Article 8(1) was engaged by the collation and retention of criminality data. They concluded definitively that it was,[19] clarifying that:

> Both [author's emphasis] the storing of information relating to an individual's private life and the release of such information come from within the scope of Article 8(1)…Even public information can fall within the scope of private life where it is systematically collected and stored in files held by authorities…This is all the more true where the information concerns a person's distant past…The data in question constitute both 'personal data' and 'sensitive personal data' for the purposes of the DPA 1998. In this regard, although data contained in the criminal record are, in one sense, public information, their systematic storing in central records means they are available for disclosure long after the event…Thus as a conviction or caution itself recedes into the past, it becomes part of a person's private life which must be respected.[20]

With Article 8(1) therefore engaged, the question to be resolved was whether the imposition into a person's private life made by the retention of the data was in 'accordance with the law'. After reviewing the extant jurisprudence on this point, the ECtHR reiterated that this means that 'the measure must have some basis in domestic law and [authors emphasis] be compatible with the rule of law'.[21] Statutory provisions necessarily satisfy the former, while the latter implies that the measure be 'accessible and foreseeable, that is, formulated with sufficient precision to enable the individual to regulate his conduct', and also 'afford adequate protection against arbitrariness and indicate with sufficient clarity the scope of discretion conferred to competent authorities'.[22]

As to whether the UK had met these requirements, the Grand Chamber made a number of pertinent points. Firstly, it noted[23] that the 1987 Recommendations relating to police held data[24] provided that open-ended and indiscriminate data collection must only be

[18] Ibid [170] [173]][176]
[19] Ibid [190]
[20] Ibid [187 – 189]
[21] Ibid [193]
[22] Ibid
[23] Ibid [196]
[24] Referred to and discussed at chapter 6.2 of this research: Council of Europe, Regulating the use of personal data in the police sector (17 September 1987), Recommendation No. R (87) 15

undertaken where specific [author's emphasis] legislation is enacted to authorise it.[25] It also noted[26] that the 1987 Recommendations provided that the duration of storage must take into account rehabilitation of offenders, spent convictions, the age of the data subject and the category of data concerned.[27] Against this backdrop, the court noted that both conviction and non-conviction data was being retained, that retention was effectively automatic and that the data was being retained until the subject was aged 100. This, said the Court, showed there to be 'no doubt that the scope and application of the system for retention and disclosure is extensive'.[28]

In light of such an extensive collection, and recognising that this may [authors emphasis] be justiciable for the purposes of criminal record checks, the court then summarised the position to be that:

> The indiscriminate and open-ended collection of criminal records is unlikely to comply with Article 8 in the absence of clear and detailed statutory regulations clarifying the safeguards applicable and setting out the rules governing, *inter alia*, the circumstances in which data can be collected, the duration of their storage, the use to which they can be put and the circumstances in which they may be destroyed. Further, the greater the scope of the recording system, and thus the greater the amount and sensitivity of the data held…the more important the content of the safeguards to be applied.[29]

The Court then finally considered whether or not there had been a violation of Article 8, considering particularly the system in operation in Northern Ireland (which largely mirrored that in England and Wales). It held that there was, because there was an

> …absence of a clear legislative framework for the collection and storage of data [and an] absence of any mechanism for independent review of a decision to retain or disclose data. The cumulative effect of these shortcomings is that there are insufficient safeguards in the system for retention and disclosure of criminal

[25] Ibid, Principle 2.1
[26] Above n.24
[27] Above n.25, Principle 7
[28] Above n.9 [198]
[29] Ibid [199 – 200]

> records data…the retention and disclosure of the applicant's caution data cannot be regarded as being in accordance with the law.[30]

The decision in *MM* resulted in Ireland passing legislation to introduce a principle of 'spent' convictions where 'spent' meant that the conviction would be retained but not disclosed as part of a criminal record check.[31] This legislative response, which effectively created a 'step-down' process similar to that created by ACPO in England and Wales in 2006, has been criticised by one commentator as a 'partial resolution'…a minimal statement of what is required which may not fully meet the requirements of Article 8 of the ECoHR'.[32]

So far as England and Wales is concerned, it is submitted that the judgment places the legality of the system of collation and retention of criminal records in England and Wales into significant question. Quite simply, it is submitted that the system is demonstrably incompliant with Article 8 because the current policy for retaining criminality data on PHOENIX involves indefinite retention of all criminality data. This must constitute a blanket retention policy and 'the blanket disclosure and [author's emphasis] retention of records violates Article 8'.[33]

Additionally, compliance with Article 8 requires that there be a 'clear legislative framework' for the collection and retention of criminal records data. While there are certainly numerous pieces of legislation relating to the disclosure of criminal records, so far as collation and retention is concerned, no such framework exists. As has been shown, the only legislative provisions for the retention of criminality data are those offered by data protection legislation,[34] s.27(4) of PACE and the various statutes relating to recordable offences outlined in chapter 3 of this research. What these provide is that the Secretary of State may by regulations make provision for recording in police national records convictions, cautions, reprimands and warnings[35] and it also provides an exhaustive list of what type of offences might be recorded but there is nothing as to the duration of

[30] Ibid [206 – 207]
[31] Per s.5 – 6 of the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016
[32] T.J. McKintyre and I. O'Donnell, 'Criminals, Data Protection and the right to a second chance' (2017) 58 Irish Jurist 27, 55
[33] R. Easton, 'The Right to be Forgotten' (2014) 178 (27) Criminal Law and Justice Weekly 408
[34] The use of this for the purpose of satisfying Article 8 so far as criminal records is concerned was considered, and rejected as insufficient, by the Court in *MM* (at [199][203])
[35] For the purposes of s.27(4), 'convictions' include cautions, warnings and reprimands. This 'clarification' was not part of the original enactment and, in fact, was only added by s.85 of the Protection of Freedoms Act 2012, presumably to rectify what had been a fairly glaring omission from the statute books up to that point.

storage, their use or circumstances in which they might be destroyed, nor does it provide any mechanism for seeking to remove data held on the PNC.

All of that is left to the police, who continue to deal with this through the issuing of guidance documents but they do not, because they cannot, provide 'a clear legislative framework' for this. The police guidance, it is submitted, is therefore insufficient for this purpose; the ECoHR in *MM* made it abundantly clear that police (and indeed Home Office) guidance alone was insufficient to satisfy Article 8(2).[36]

The decision in *MM*, which is merely persuasive in England and Wales, has not permeated into domestic jurisprudence as perhaps might be hoped. Arguably the leading authority in domestic law which offers a consideration of *MM* is *R (on the application of Catt) v Commissioner of Police of the Metropolis and another*.[37] *Catt* was not strictly speaking a 'criminal records' case; rather, it involved a complaint that a record had been created on the 'National Domestic Extremism Database' which referred to the political activities of a 91 year old 'peace activist' appellant who had been arrested twice, but not charged with any offence. Although not himself subject to a nominal listing on PHOENIX, his name appeared in the nominal records of two other data subjects who were listed on PHOENIX.[38]

Despite accepting that 'things have moved on' since the decision in the *Five Constables* case and that there was 'no longer any doubt as to the applicability of Article 8 on the systematic retention of processible personal data',[39] the Supreme Court then, it is submitted, made precisely the same errors that the Court of Appeal did in that earlier judgment. It heard anecdotal evidence from police officers as to the 'operational value' of the data held, and accepted this almost *prima facie* as being justification for retaining the data for 'the protection and detection of crime'.[40] The Court referred the appellant to the viability of making a complaint to the Information Commissioner under the DPA 1998,[41] even though such a complaint surely would have fallen on stony ground in light of the decision in *Five Constables* case.

[36] Above n.9 [203]
[37] [2015] UKSC 9
[38] Ibid [18] [22]
[39] Ibid [16]
[40] Ibid [29 – 30]
[41] Ibid [34]

Moreover, the Court then made, it is submitted, two fundamental errors of applicability as regards the decision in *MM*. The first was to make the critical error which continues to permeate this area of data protection law and to deal with retention of personal data as inexplicably linked to its use and, more specifically, the disclosure of it. In *MM*, as outlined above, the two issues were (it is submitted, correctly) treated as interlinked, but separate, issues; that is to say that the simple retention of criminality data must be 'in accordance with the law' on its own merits. The Supreme Court did not seem to agree, and distinguished the instant case with *MM* on the grounds that:

> There has been no disclosure to third parties, and the prospect of future disclosure is limited by comprehensive restrictions. It is limited to policing purposes, and is subject to an internal proportionality review and the review by the Information Commissioner and the courts.[42]

This analysis fails in three regards. Firstly, this type of information is precisely the kind which is liable to be disclosed as part of the discretion permitted to chief officers in the issuing of an enhanced DBS certificate,[43] so is perfectly disclosable to third parties in certain circumstances and therefore not strictly limited to 'policing purposes'. Secondly, the Information Commissioner has no authority to enforce any possible data breach invoked by the retention of this type of criminality data because s/he is bound by the *Five Constables* decision and, thirdly, the Courts are equally bound by the decision in that case until or unless an appellate court overrules it. All of that notwithstanding, there is nothing in *MM* which indicates that this is a pertinent, let alone the distinguishing, determining factor in considering whether data collation and retention is of itself is 'in accordance with the law'.

The second error of applicability, it is submitted, was that the Court erred in accepting that the various piecemeal statutory provisions outlined above, and the applicable guidelines supplementary to them, were sufficient to satisfy the requirement outlined in *MM* that there must be a 'clear and detailed statutory regulations clarifying the safeguards applicable and setting out the rules' governing the storage of data generally, and particularly criminality data. This was justified, without any reference to any legal authority, as being

[42] Ibid [15]
[43] A fuller examination of these is offered below and at C. Baldwin, 'Necessary intrusion or Criminalising the Innocent? An exploration of modern criminal vetting' (2012) 76 (2) Journal of Criminal Law 140

because ‘the rules do need not be statutory, provided that they operate within a framework of law and that there are effective means of enforcing them’.[44] It is difficult to reconcile that position with that in *MM*; indeed, it appears to be a rather clear and contradictory misapplication of it.

It is perhaps little wonder that one commentator later lamented that the decision in *Catt* was ‘rather frustrating, particularly bearing in mind the non-statutory nature of the database and the criticisms made in *MM*’[45] while another suggested that ‘perhaps there is a need for a Police Ombudsman in England and Wales to whom parties might appeal on such questions in a timely and cost-free manner, rather than use the courts. The current policy seems to give a great deal of discretion to the police – perhaps too much? [If appealed] It would not be surprising if the ECtHR took a less flexible view’.[46]

Whatever the merits of creating an independent body with (presumably) statutory powers to oversee the use of criminality data by the police, what remains unclear is why, in light of the continuing judicial reticence to apply fully the principles enunciated in *MM*, Parliament has not legislated on this issue. Perhaps it remains the case that Parliament (and indeed the judiciary) prefer to give the police ‘the whip hand’ on matters which they consider to be police operational issues,[47] and this has resulted in a ‘broad discretion in relation to the retention of data about both convicted criminals and those who are merely suspects’,[48] but it is submitted that it is now time for Parliament to legislate. It would not only ensure compliance but would also give Parliament a welcome, and it is submitted, long-overdue opportunity to debate the issue properly.

The suggestion that the retention, storage and use of criminality data is due Parliamentary consideration and legislation is a long-standing proposition; in the IT decision which preceded the *Five Constables* appeal, the IT commented that, so far as the expanding use of criminality data on the PNC was concerned:

---

[44] Ibid [11]
[45] M. Oswald, ‘Joining the dots – intelligence and proportionality’ (2013) 13 (5) Privacy and Data Protection Journal 6
[46] H. Johnson, ‘Data Retention – scope of police powers’ (2015) 2 Communications Law 56, 58. In January 2019, the ECtHR did precisely that and found a violation against Mr. Catt. This is analysed in brief in the next chapter of this research.
[47] See the lead pronouncements in the *Five Constables* case and also H. Johnson, ‘Data Retention – scope of police powers’ (2015) 2 Communications Law 56, 58
[48] Ibid, 56

> If the government wishes the PNC to have that role then it needs to legislate accordingly. This would provide the opportunity for Parliamentary debate as to how best to provide an appropriate and proper legislative framework so that there is a clear understanding of data ownership and obligations with proper safeguards.[49]

That proposition was rejected in the *Five Constables* appeal by Waller LJ, who claimed that 'I see no reason why it needs to be authorised by specific legislation. The Data Protection Act 1998 already provides an appropriate framework, in accordance with the Directive, for regulating data ownership and providing proper safeguards'.[50] This approach was expressly that rejected by the ECtHR in *MM* and it is submitted, therefore, that it is now time for the legislature to conduct that reconsideration in full.

9.4 The ECtHR rejection of unfettered police powers regarding the collation and storage of biometric criminality data

As has been illustrated in chapter two of this research, the police collection of criminality data has never consisted solely of collating and storing data relating to offences, suspects and convicted individuals. The police have for centuries also retained extensive collections of photographs, fingerprints and, more recently, bodily samples, including DNA (collectively now referred to as 'Biometric Criminality Data', or 'BCD'), which were intrinsically linked to the 'bare' criminal record data to provide a fuller picture of each individual listed.

For almost the entirety of that collection, as with the 'criminal records' data now stored on PHOENIX, the police have enjoyed an almost unfettered discretion on what they might collect, store and retain. The same permissive PACE provisions which authorised the collection of criminal records, also authorised the collection of fingerprints and other samples[51] which might be retained indefinitely if the suspect was convicted but which had to be destroyed if a person was not subsequently convicted of the offence[52] but no further guidance on the collation or storage of this data was provided.

---

[49] The Chief Constable of Humberside (and four others) v The Information Commissioner, Information Tribunal Appeal Numbers EA/2007/0096, 98, 99, 108, 127 (21 July 2008) [99]
[50] [2009] EWCA Civ 1079 [66] This position should be contrasted with that offered by Hughes LJ, who suggested that amendments could conceivably be made to the regime, but that 'none of that is for me. It is for Parliament' [112]
[51] Per ss.61 – 63 of the Police and Criminal Evidence Act 1984, as originally enacted.
[52] Per s.64, ibid.

The police penchant for ignoring the requirement to delete PHOENIX data in a timely manner also seemed to have permeated their approach to their BCD repository. This became apparent in May 2000 when DNA was used to implicate two separate individuals to a rape and a murder respectively; however, both convictions were overturned on appeal because the DNA samples which had linked them to the offences had been unlawfully retained after acquittals in prior investigations.[53] Rather than admonish the police, Parliament instead elected to legislate to significantly expand the retention powers of the police as regards BCD in 2001 so that these could be taken from anyone arrested in connection with a recordable offence and subsequently retained indefinitely by police for use in crime detection, prevention, investigation and prosecution.[54]

In a similar vein to those who complained to the Information Commissioner about the indefinite retention of their PHOENIX data, the new legislative provisions gave almost immediate rise to complaints from individuals who objected to their BCD being indefinitely retained. The issue was ultimately considered by the House of Lords in 2004 after two individuals challenged the police retention of their BCD despite the conclusion of prosecutions against them which did not result in convictions.[55] The Judicial Committee ruled unanimously that the provisions were not contrary to Article 8 and that the samples could be retained. Indeed, only Baroness Hale believed that the collation and retention of such criminality data even engaged Article 8,[56] but in any event that the collation of a 'DNA database' was justified because the 'whole community, as well as individuals whose samples are collected, benefits from there being as large a database as it is possible to have'.[57] The analogy with the police criminality data collection on PHOENIX is self-evident, where an almost identical approach can be, and indeed has been, taken.

However, in a widely-publicised judgment, that position was disapproved by the Grand Chamber of the ECtHR in 2008.[58] Here it was noted that the United Kingdom was the only signatory state which permitted the near automatic collation, and indefinite retention, of all

[53] *R v Weir* (26 May 2000) CA (Crim) and *R v D (Attorney General's reference No.3/1999)* [2001] 2 AC 91
[54] Per s.64(1A) of the Police and Criminal Evidence Act 1984, inserted by s.82 of the Criminal Justice and Police Act 2001.
[55] *R (on the application of S) v Chief Constable of South Yorkshire, R (on the application of Marper) v Chief Constable of South Yorkshire* [2004] UKHL 39 [11 – 12]
[56] Ibid [73]
[57] Ibid [78]
[58] *S and Marper v UK* [2008] ECHR 30562/04

BCD for both convicted and acquitted persons.[59] The Court affirmed that the mere storage of data relating to the private life of an individual amounts to an interference for the purposes of Article 8(1) and that the subsequent use of that data is only instructive as to whether 'private life' aspects are being adversely affected.[60] Both cellular and DNA samples are 'personal data' for the purposes of the Data Protection Act 1998 where they are held by those who might identify individuals from them[61] and the retention of these constitute an interference with Article 8 rights.[62] The same determination was made in respect of fingerprints.[63]

The question was, therefore, whether Article 8(2) might justify the interference. After considering the Lady Hale's proposition that the public interest in retaining information which assisted in crime prevention and detection against the rights of individuals under Article 8(1), the Court held that it did not and that a violation of Article 8 had occurred.[64] The *ratio decidendi* of that decision, which has been oft cited subsequently, was that:

> the Court is struck by the blanket and indiscriminate nature of the power of retention... The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender [and where an individual is] arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time-limited…Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the nationwide database of the materials; in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances.[65]

The similarities between the *ratio* for finding the regime for collating, storing and retaining BCD in *S and Marper* as unlawful and that cited in respect of the collating, storing and retaining of criminal record data four years later in *MM* are striking. In both cases the Court

[59] Ibid [47 – 48]
[60] Ibid [67]
[61] Ibid [69]
[62] Ibid [77]
[63] Ibid [86]
[64] Ibid [126]
[65] Ibid [119]

recognised that the mere storage of such data amounted to an engagement of Article 8, that the indefinite and blanket retention of such data constitutes an unjustifiable interference with private life, that the absence of an independent review to challenge the retention further exacerbates the unjustifiable interference, as does the failure to make accommodations to retention periods commensurate to the seriousness of the offence to which the data relates. In short, the Grand Chamber appear to have applied a near identical set of factors as a means of testing the legality of the collation and storage of BCD as they did four years later to criminal conviction data. This, it is submitted, shows that the Grand Chamber were elucidating principles of general applicability, rather than anything particular to specific datasets and databases.

What followed, then, is also of some considerable interest. In direct contrast to the complete inertia which has followed the decision in *MM*, Parliament responded to the decision in *S and Marper* by introducing primary legislation to significantly amend the PACE retention regime for collating, storing and retaining BCD. Part 1 of the Protection of Freedoms Act 2012, which came into force on October 31 2013, inserted 63D into PACE 1984 and created a new, prescriptive and far more restrictive statutory regime for the retention and destruction of BCD. The overarching provision was that BCD may still be obtained where an individual is arrested for a qualifying offence but that it must subsequently be destroyed unless any of the exceptional circumstances laid down in ss.63E – 63P are met.[66]

These 'exceptional circumstance' provisions created statutory retention periods for BCD. Any BCD lawfully obtained and stored by the police on the National DNA Database ('NDNAD') must now be deleted immediately after an investigation into a minor offence concludes without the suspect being convicted,[67] and likewise where a voluntary sample is provided but which results in no conviction.[68] Where an individual is arrested in connection, but not charged, with a qualifying offence,[69] BCD can only be retained for

[66] Per s.63D(3) of the Police and Criminal Evidence Act 1984, as inserted by s.1 of the Protection of Freedoms Act 2012
[67] Per s.63H of the Police and Criminal Evidence Act 1984, as inserted by s.4 of the Protection of Freedoms Act 2012.
[68] Per s.63N(2) of the Police and Criminal Evidence Act 1984, as inserted by s.10 of the Protection of Freedoms Act 2012.
[69] Per s.63F(5)(6) of the Police and Criminal Evidence Act 1984, as inserted by s.3 of the Protection of Freedoms Act 2012.

three years if authorised by the Biometric Commissioner,[70] with a potential extension of a further two years only after obtaining an order from District Judge.[71] Similarly, where an individual was charged with, but not convicted of, a qualifying offence, a three year retention period applied,[72] though this could be extended by a further two years if permitted by a District Judge.[73]

BCD obtained as part of a PNfD must be deleted after two years,[74] while data obtained during the successful prosecution of a juvenile for a minor offence can be retained for five years.[75] A 'minor offence' for this purpose is one where the individual receives a custodial sentence of less than five years.[76] However, all BCD is still retained indefinitely where any person is arrested or charged with any qualifying offence after having been previously convicted of any recordable offence,[77] irrespective of the disposal in the earlier matter, or where a juvenile is convicted of a qualifying offence[78] or where an adult is ultimately convicted of any recordable offence.[79]

These provisions are instructive in a number of respects. They are a clear and direct attempt to rectify at least some of the criticisms of the BCD system made in *S and Marper* (which were later made in almost identical terms in *MM*). Parliament provided differing retention periods based on the gravity of the offence to which the material relates, the age of the offender and the strength of the allegations made against them (noting the

[70] The new post of 'The Commissioner for the Retention and Use of Biometric Material' was created by s.20 of the Protection of Freedoms Act 2012 and his remit bears a more than striking resemblance to that of the Information Commissioner in their respective data fields. The Biometric Commissioner offers oversight to the use of biometric data, an avenue of complaint in the event of a dispute and s/he produces annual reports to Parliament (per s.21 of the Protection of Freedoms Act 2012).
[71] Per s.63F(7) of the Police and Criminal Evidence Act 1984, as inserted by s.3 of the Protection of Freedoms Act 2012.
[72] Per s.63F(5)(6) of the Police and Criminal Evidence Act 1984, as inserted by s.3 of the Protection of Freedoms Act 2012.
[73] Per s.63F(7)(9) of the Police and Criminal Evidence Act 1984, as inserted by s.3 of the Protection of Freedoms Act 2012.
[74] Per s.63L(2) of the Police and Criminal Evidence Act 1984, as inserted by s.8 of the Protection of Freedoms Act 2012.
[75] Per s.63K(1)(4) of the Police and Criminal Evidence Act 1984, as inserted by s.7 of the Protection of Freedoms Act 2012.
[76] Per s.63K(2) of the Police and Criminal Evidence Act 1984, as inserted by s.7 of the Protection of Freedoms Act 2012.
[77] Per s.63F(2) of the Police and Criminal Evidence Act 1984, as inserted by s.3 of the Protection of Freedoms Act 2012.
[78] Per s.63K(3) of the Police and Criminal Evidence Act 1984, as inserted by s.7 of the Protection of Freedoms Act 2012.
[79] Per s.63I(1)(2) of the Police and Criminal Evidence Act 1984, as inserted by s.5 of the Protection of Freedoms Act 2012.

distinction between those arrested but not charged, and those charged but not convicted, specifically).

This can be directly contrasted to the regime for data held on PHOENIX, where there is absolutely no differentiation made whatsoever between material relating to conviction and non-conviction data, the gravity of the allegation (or conviction) made against the data subject or the age of the subject of the Nominal Record. Everything is simply retained until the suspect reaches age 100 years. A juvenile given a simple caution for a shop-theft will have his BCD deleted after five years. His Nominal listing, however, will remain until s/he reaches 100 years of age. This significant divergence in retention period is difficult to reconcile, particularly noting that the failure to provide this kind of differentiation was the reason why such a 'blanket collection and retention' regime was unlawful in *MM*.

It is submitted that Parliament's willingness to legislate to accommodate such a regime as regards BCD, but not as regards the PHOENIX criminality data, is therefore clearly unsatisfactory. Quite simply, if retention periods need be varied regarding BCD because a blanket retention regime is disproportionate, it is difficult to understand why such a position (which in effect remains *in situ*) is acceptable so far as the PHOENIX data is concerned. In fact, it might reasonably be supposed that the early deletion of BCD might be more prejudicial to crime detection and public protection than the deletion of PHOENIX data; the linking of suspects to historical offences by DNA and fingerprints many years later seems a far more plausible and useful application of criminality data than holding some aged and merely textual information relating to an offender in an Event History section of a nominal listing.

Additionally, BCD may be more 'intrusive', so far as the raw data itself is concerned, but it is difficult to envisage it being used for anything other than policing and criminal justice purposes. PHOENIX data, by contrast, has a potentially far more 'intrusive' impact on the data subject, both by its permanency and particularly in its use for vetting purposes outwith the criminal justice sphere. BCD will rarely, if ever, be disclosed to third parties and any use of it subsequent to the instant criminal proceedings will almost always take place without the knowledge of the data subject. PHOENIX data has neither of these characteristics; it is widely used and disclosed to numerous authorised bodies, to employers and to voluntary groups and the data subject will be routinely aware that it is being so used whenever they are required to apply for a visa or a criminal record check.

It is, therefore, submitted that the application of near identical principles laid down by the ECtHR to two separate, yet intrinsically intertwined, collections of criminality data reveal and highlight the wide discrepancy in the way which that data is treated in England and Wales which do not appear to stand well to close scrutiny. Parliament, as part of any legislative reconsideration of PHOENIX, might therefore wish to consider that a more consistent approach be taken to more accurately reflect the authority laid down in the European jurisprudence, the nature and use of the data itself and the likely impact of that retention on the individual data subject.

9.5 Does *S and Marper* and *MM* apply only to the unconvicted?

What is also notable is that, like the police retention guidelines for PHOENIX, the BCD legislative regime offers little prospect of deletion for those convicted of an offence. For the purposes of BCD, cautions, reprimands and warnings take the meaning ascribed to them by s.27(4) PACE[80], so that they are considered to be analogous to 'convictions'.

Notwithstanding the legal contradiction inherent to that position,[81] it is not immediately apparent why Parliament has drawn such a marked distinction between data held relating to convictions and that of those not convicted. It appears that they have taken their lead from jurisprudence. In the *Five Constables* case, the applicability of the principles set down in *S and Marper* was raised by the Information Commissioner but this was shortly rebuffed; Waller LJ dismissing it on the basis that he believed that the latter case involved only a 'particular concern' regarding the retention of criminality data relating to 'the unconvicted'.[82] This position is further reflected in the Parliamentary debates which led to the implementation of the BCD regime, where the (then) Home Secretary Theresa May told the Commons during the second reading of the Bill that 'we will be taking innocent people off the DNA database and putting guilty people on'.[83]

It is submitted that the presumption that the *S and Marper* and *MM* principles apply only to the unconvicted is not correct. Certainly, there is nothing in the judgment to indicate that the principles apply only to the unconvicted and the appellant in *MM* had, in fact, been

[80] National Police Chief's Council, 'Deletion of records from national police systems (PNC/NDNAD/IDENT1)' (18 October 2018) 5, para.2.3.3
[81] See chapter 3 of this research for further analysis on this point
[82] Above n.2 [80]
[83] HC Deb 1 March 2011, vol.524, col.205

cautioned and her appeal was ultimately decided in her favour based on those principles. In *R (on the application of F) and Thompson v the Secretary of State for the Home Department*[84] the Supreme Court, in determining that indefinite notification requirements for convicted sex offenders were a disproportionate interference with Article 8 rights, certainly seemed to suggest that the principles did not apply just to the unconvicted.

In fact, the rationale for their decision was based largely on the decision in *S and Marper*, which was applied throughout. This focused on the lack of any right to review the notification requirement (described as 'highly relevant to the question of compliance with Article 8')[85] and also on the disproportionality resultant from the presumption that all of those convicted posed a life-long, continuous risk of re-offending despite there being almost no empirical support for the proposition. Indeed:

> If some of those who are subject to lifetime notification requirements no longer pose any significant risk of committing further sexual offences and it is possible for them to demonstrate that this is the case, there is no point in subjecting them to supervision or management or to the interference with their Article 8 rights …Indeed subjecting them to these requirements can only impose an unnecessary and unproductive burden on the responsible authorities…No evidence has been placed before this court or the courts below that demonstrate that it is not possible to identify from among those convicted of serious offences … some at least who pose no significant risk of re-offending.[86]

It seemed that the principles set down in *S and Marper*, and therefore by extension, *MM*, applied even to those convicted of the most grievous, sexual offences. It was, therefore, something of a surprise when the Supreme Court handed down its judgment in *Gaughran's Application for Judicial Review,*[87] which involved a review of BCD obtained by the police in Northern Ireland under the (near identical) Northern Irish equivalent of the statutory BCD retention provisions when a man was convicted in court of a drink driving offence, fined £50 and given a twelve month driving suspension and found that his BCD would be held indefinitely.[88]

---

[84] [2010] UKSC 17
[85] Ibid [34] (Lord Phillips)
[86] Ibid [51] [56]
[87] [2015] UKSC 29
[88] Ibid [1]

After accepting that Article 8(1) was engaged[89] Lord Clarke, giving the lead judgment of the majority of four, then asserted that the interference was 'in accordance with the law' because it was proportionate. He found as such on several grounds. Firstly, it was asserted that the delineation marker of retention for all recordable offences to be 'sufficient to meet the requirement that consideration be duly given to the nature of the offence'.[90] Secondly, he also found that, although there was no process of review, this did not matter much, because it was said that 'very few states have a process of review'.[91] Notwithstanding that multiple breaches of the ECoHR do not give rise to a defence to an action brought under it, it is not at all clear where this information comes from; certainly an article[92] cited by the Court as 'evidence' to this point does not support such a finding.

Moreover, Lord Clarke further asserted that the decision in *S and Marper* cannot apply because 'the ECtHR was not considering the position of convicted people'[93] and indeed there was 'no indication that the Strasbourg Court was considering the position of those who had been convicted at all'.[94] This, it is submitted, is an erroneous proposition which fatally undermines the judgment. Jurisprudence subsequent to *S and Marper*, (even if that in *MM* and *R(F)* are excluded, which are difficult to reconcile so excluding) clearly shows the applicability of the principles posited as equally applicable to those with criminal convictions. In both *W v Netherlands*[95] and in *Peruzzo v Germany*[96] the ECtHR applied almost identical considerations to the provisions for the retention of criminality data relating to convicted persons in the respective member states, and in each the Court applied *S and Marper* directly in assessing whether the provisions were Article 8 compliant. In *Peruzzo*, particularly, the difference between the unconvicted and convicted was noted[97] but only as one factor which the court took into account before considering all of the others laid down in *S and Marper*.

[89] Ibid [19]
[90] Ibid [34]
[91] Ibid [43]
[92] Santos et al, 'Forensic DNA databases in European countries: is size linked to performance?' (2013) 9 Life Sciences, Society and Policy 12
[93] Above n.88 [29]
[94] Ibid [31]
[95] 20689/08, 20 January 2009
[96] (2013) 57 E.H.R.R SE17
[97] Ibid [44]

Ultimately, the system in Germany was declared lawful because it contained a periodic, ten-year process of independent review,[98] it only retained BCD on those convicted of an offence of 'a certain gravity' (and these included only the more serious offences, as contrasted to English equivalent of 'recordable offences') or where a pattern of offences showed that the 'certain gravity' threshold was reached, whether there are sufficient grounds to suspect that the offender will commit future offences, in light of 'the circumstances of a particular case, the personality of the convict' and reasons must be provided explaining why future proceedings in each individual case are assumed.[99] The existence of a viable route for legal challenge was also highlighted as a determining factor.[100]

It is these safeguards which prevent the German system being considered a 'blanket and indiscriminate' system[101] of the type identified in the UK in *S and Marper* and, indeed, in *MM*, which prevented there being a disproportionate interference with Article 8 rights. Each of these is plainly missing from the system in the UK, even under the amended version for BCD created by the 2012 revisions.

Each of these is also plainly missing from the system of retaining criminality data on the PHOENIX database, which, it is submitted, therefore still constitutes nothing less than a 'blanket and indiscriminate system' as described in the relevant jurisprudence. What is evident, it is submitted, is that the principles in *S and Marper* do, in fact, apply to the convicted, albeit that the fact of conviction itself will be a relevant factor to consider, rather than the determining factor. This view is shared by Coghlan, who provides simply that 'there is no support for *Gaughran's* view that the principles in *S and Marper* do not apply to the convicted'[102] and that 'it is likely that Strasbourg will find a violation in *Gaughran*'.[103] Reed, meanwhile, postulates that 'the retention net is cast perhaps rather wider than is necessary' and that the threshold of recordable offences is 'a low one',[104] while Johnson

[98] Ibid [46]
[99] Ibid [44]
[100] Ibid [47]
[101] Ibid
[102] N. Coghlan, 'Gaughran [2015] UKSC 29 on biometric data retention: Strasbourg unheard, Strasbourg unheeded' (2016) 1 European Human Rights Law Review 61, 67
[103] Ibid, 72. Coghlan's treatment of the decision in *Gaughran* is an extremely detailed and persuasive piece which details the problems inherent in that judgment far more expansively than is necessary in this research.
[104] K. Reed, 'Retaining DNA' (2015) 179 Criminal Law and Justice Weekly 514

simply comments that, so far as the Supreme Court view that the interference is proportionate and so justified, 'one doubts that the ECtHR will agree'.[105]

The *Gaughran* judgment has been appealed to Strasbourg and the decision of the ECtHR is likely to be handed down very soon after the completion of this research. It is not difficult to imagine that the Court are likely to find an Article 8 breach, and it is to be hoped that it will take the opportunity to clarify, definitively, whether there is a distinction to be drawn in the principles which apply to criminality data pertaining to the convicted and those who are not, and, if so, what that distinction is. The applicability of such a judgment to the PHOENIX data is obvious, and potentially very welcome.

9.6 The developing challenge to the police hegemony on custody image data.

Although the collection of photographs to accompany the 'criminal records' can be traced to the nineteenth century, no formal statutory provision authorising the collection, storage and retention of custody images was enacted until s.64A was inserted into PACE by s.92 of the Anti-terrorism, Crime and Security Act 2001 which permitted the taking of custody photographs (or video recording)[106] of any person arrested for an offence[107] or issued a fixed penalty notice.[108] The statutory provisions provide an almost identical justification for use as those for BCD[109] and that 'after being so used or disclosed, images may be retained but may not be used or disclosed except for a purpose so related'.[110] Custody images are now stored on local police systems and uploaded from these to the Police National Database ('the PND'), rather than PHOENIX.[111]

[105] Above n.47
[106] Per s.64A 6(A) of the Police and Criminal Evidence Act 1984, as inserted by s.116(5) of the Serious Organised Crime and Police Act 2005.
[107] Per s.64A (1B)(a) of the Police and Criminal Evidence Act 1984, as inserted by s.92 of the Anti-terrorism, Crime and Security Act 2001
[108] Per s.64A (1B)(d – e) of the Police and Criminal Evidence Act 1984, as inserted by sch.12, para.7(3)(b) of the Policing and Crime Act 2017
[109] Per s.64A (4) of the Police and Criminal Evidence Act 1984, as inserted by pt.3 s.116(3) of the Serious Organised Crime and Police Act 2005
[110] Per s.64A (4)(b) of the Police and Criminal Evidence Act 1984, as inserted by s.92 of the Anti-terrorism, Crime and Security Act 2001
[111] Home Office, 'Review of the use and retention of Custody Images' (February 2017) 2, para.1.2

The legislation was silent as to retention periods other than that custody images 'may be retained'.[112] This led Michael Zander to comment that 'the words appear to mean that they may be retained indefinitely, regardless of the outcome of the case'.[113] Whether this reading was correct or otherwise, general guidance on the overarching principles relating to the collection, management, sharing and retention of police information was provided by a Home Office Code of Practice,[114] issued in accordance with the relevant statutory enabling provisions,[115] but the more detailed provisions were provided by the supplementary Guidance on the Management of Police Information ('the MOPI Guidance'), issued firstly in April 2006, then in revised form in 2010.[116]

It is perhaps worth noting that the MOPI Guidance is produced by the police, for the police – it is precisely the sort of internal policy document that the police have relied on for decades to 'manage' their collections of criminal records. That notwithstanding, the MOPI Guidance provides general principles of police data retention. The first two editions contained nothing specific relating to custody photographs, but instead provided a general system of categorisation which police forces were presumed to apply to them. 'Category 1' offences, subtitled 'certain public protection matters', related to any allegation, proven or otherwise, of murder or any other 'serious offence' as specified in the Criminal Justice Act 2003, a 'potentially dangerous' person or any information relating to an individual who had been managed under a MAPPA. Such information, though scheduled for automatic police review every ten years to ensure relevance and that records are up-to-date, would be kept, similar the PHOENIX records, until the named individual reached age 100 years unless there were 'exceptional circumstances' to delete it.[117]

Other information was divided into two main further categories. 'Category 2' offences were 'other sexual, violent or serious offences'. Data relating to these was to be retained until the offender was no longer judged to pose any risk of harm. This was to be judged by a chief officer review of the information at each ten-year clear period. If a risk was thought

[112] Per s.64A(1) of the Police and Criminal Evidence Act 1984, as inserted by s.92 of the Anti-Crime, Terrorism and Security Act 2001.
[113] M. Zander, 'The Required Destruction of Custody Photographs', (2012) 176 Criminal Law and Justice Weekly 489
[114] National Centre for Policing Excellence, 'Code of Practice on the Management of Police Information' (July 2005)
[115] Per s.39A of the Police Act 1996
[116] National Policing Improvement Agency, 'Guidance on the Management of Police Information' (2nd edn, 2010)
[117] Above n.114, 93

to still exist, the data would be retained and the cycle restarted.[118] All other records were considered 'Category 3' and the guidance proposed that these 'do not necessarily have to reviewed' but that forces might optionally elect to dispose of these on a time basis if the cost of maintaining them outweighed the risk of disposal. Any force which elected to have a time-based review must retain these records for at least six years.[119]

The contrast with the policies for retaining PHOENIX data are once more instructive, at least in a theoretical context. Unlike the PHOENIX data, which is simply collated and stored automatically regardless of the nature of the criminality in question, here the police implemented a general system of police data management which offered differentiated retention periods and processes based predominantly on the seriousness of the alleged offence and the potential risk of harm posed by the data subject. There are also elements of discretion offered, with individual chief constable data controllers being advised to implement their own policy regarding 'Category 3' data based on their own operation needs and with an almost tacit acceptance that the cost of maintaining data related to low level, low risk criminality might outweigh the benefits of retaining it. Additionally, there was a review system, albeit an internal rather than independent one, for most of the data being held, with specified time-frames stipulated.

These differences, however, were almost certainly more theoretical than practical. One potential alternative reading of the MOPI guidance was that the police had the potential to retain all data in all circumstances; a chief constable may believe that all 'Category 2' subjects remain a potential risk at each ten-year clear period review (and so their data is retained) and they may also determine that the cost of 'Category 3' retention is not outweighed by the 'operational benefit' offered by the data, so no review or disposal of such data would be necessary (and so all images are retained). In light of the police fondness for retaining criminality data generally, it is likely that data was retained for lengthy periods in all cases and it is not, therefore, perhaps surprising that a judicial challenge to the retention of custody images was eventually brought against the police.

In *R (on the application of RMC) v Metropolitan Police Commissioner,*[120] claims were brought by two individuals whose custody images and BCD had been obtained, and

[118] Ibid 94
[119] Ibid 94 – 5
[120] [2012] EWHC 1681

subsequently retained, by the police after they were arrested in connection with an offence. In the case of RMC, a woman of good character was arrested on suspicion of assault occasioning actual bodily harm against a community support officer who had stopped her cycling on a footway.[121] In the case of FJ, a fifteen year old boy was arrested on suspicion of raping his second cousin.[122] Neither individual was ultimately charged with an offence. In both cases, the police elected to retain BCD and custody images (and, in the case of FJ, to add an 'Event History' to PHOENIX) which the police refused to delete when asked to do so.[123]

It was accepted by the applicants that the relevant provisions of PACE permitted the police to retain the photographs, so the basis of the judicial review application was that the continued retention of them under PACE was a breach of Article 8 because Article 8(2) was not satisfied as such retention was not 'in accordance with the law'.[124] After noting the aforementioned MOPI provisions which governed the retention of custody images,[125] Richards LJ considered the evidence provided by the police as to how those guidance documents were implemented in practice. He found a 'confused picture', with senior officers claiming to make decisions concordant with the MOPI Guidance but whose internal processes and documentation did not explicitly refer to them.[126] He also noted that, in evidence provided by the decision-making officer, no mention was made of the MOPI guidance at all. This, said the court, was 'a surprising omission',[127] though this might have been perhaps less so had the Court thought to consider the police's somewhat lackadaisical attitude to following their own weeding guidance regarding their PHOENIX data collection.

It was also noted that the police response to the solicitor's letter sent by RMC's representative took 'a long time' and even then 'the retention of photographs was not dealt with'. This, it is submitted, might perhaps suggest a procrastination on the part of the data controller. It might also perhaps suggest that the police were emboldened by their success in the *Five Constables* case to believe that the Courts would continue to defer to their 'operational needs', so far as data collection was concerned. When asked to address the

[121] Ibid [4]
[122] Ibid [5]
[123] Ibid [4 – 5]
[124] Ibid [8]
[125] Ibid [10 – 17]
[126] Ibid [18]
[127] Ibid [24]

issue in evidence, Commander Gibson gave evidence that 'I do not accept the argument that no policing purpose is served by the retention of the information'.[128] No further elaboration, exposition or evidential basis for this point was made. In FJ's case, responses were quicker, but all requests for deletion were steadfastly refused.[129]

This was because, even had the Guidance been followed, then the categorisation of these 'offences' (as Category 2 and 1 for each applicant, respectively), meant that RMC's custody images would have been held for at least six years, with periodic reviews every ten, while FJ's data would be held until he was aged 100 years. In essence, therefore, the real question wasn't whether the guidance had been properly followed (though, it is submitted and indeed as was heavily inferred throughout the judgment, it almost certainly was not) but whether the guidance itself was sufficient to meet the requirements of Article 8(2).[130]

As to whether the question need be asked at all, because Article 8(1) was engaged, the court found that, applying the principles enunciated in *S and Marper*, 'it is plain that the ECtHR considers that the retention of photographs in police records engages Article 8'.[131] This is because 'the photographic images go further than simply displaying physical appearance at a particular age: they disclose that [s/]he was in police custody…Thus they contain, and convey, both his physical appearance *and* [original emphasis] the fact of police arrest and detention'.[132] Once more, then, the question fell as to whether such an interference might be justified by reference to Article 8(2) ECoHR.

After accepting that s.64A PACE had to read in parallel to the MOPI code (even if it was not actually followed by the police)[133] and that a finding that the police failure to reference the MOPI Code directly in their own decision-making processes might be sufficient to find an unjustified interference but could be easily rectified and offer no actual relief to either applicant (which would be 'deeply unsatisfactory')[134] the Court ruled that the retention

[128] Ibid [22]
[129] Ibid [21]
[130] Ibid [25]
[131] Ibid [33]
[132] Ibid [37]
[133] Ibid [45]
[134] Ibid [46]

policy under the MOPI guidance was sufficiently disproportionate as to constitute an unlawful interference under Article 8.[135]

This was because the provisions 'did not strike a fair balance between the competing public and private interests and meet the requirements of proportionality'.[136] Although 'more structured' than the system considered in by the ECtHR in *Marper*, the MOPI guidance still drew 'bright-lines' which did not sufficiently distinguish between the convicted, those charged but acquitted and those not charged at all, that retention periods were 'on any view for a long period, is likely to be in practice much longer and potentially indefinite' and makes no provision for the age of those photographed.[137]

The judgment in *RMC* follows an almost identical path to that taken in *S and Marper* and *MM*. There is a police determination to retain their unfettered discretion to collate and retain whatever criminality data they wish. There is an insistence, uncorroborated by any empirical evidence whatsoever, that such data is required to allow them to perform 'core' crime prevention and detection functions. There is an apparent presumption that anyone who comes to police attention does so because they are likely criminal and, therefore, they should be treated as a potential suspect for at least a very long time, or, more probably, until they die or are so old as to be highly unlikely to 'offend again'.

There is a reliance on documented guidance procedures which *prima facie* provide for review and appeal against data retention but which, in reality and exactly like the police weeding guidance documents, were little more than obfuscatory devices intended to convey an illusion of data protection and human rights compliance. In practice, the policies had little or no relevance to police decision making processes. That notwithstanding, the guidance policies themselves made no distinction between the convicted and those who are not or the juvenile and the adult. The police position was made, once more, in vain. Once more it was heavily criticised by the Court and ultimately declared unlawful by direct application of the principles in *Marper* to another set of police held criminality data; the unfettered discretion was to be removed and the indiscriminate and indefinite retention of data was to end.

[135] Ibid [55]
[136] Ibid
[137] Ibid [54]

The decision in *RMC* reached the wider public consciousness as it was routinely reported in national news media.[138] The judgment was expected to trigger an expedient change in retention of custody images; Richards LJ had warned the police that he expected a new, Article 8 compliant policy to be formulated and implemented 'in months, not years'.[139] His warning was in vain. It wasn't until October 2014 that further MOPI guidance, which superseded the 2010 Guidance,[140] was published but the new policy made no changes whatsoever to the retention regime for custody images.

In fact, the police appeared to be ignoring entirely the decision in *RMC* and were by 2014 in an advanced stage of uploading every one of their custody photographs to the PND with the express intention of creating a searchable, facial recognition database. This state of affairs so alarmed Alastair MacGregor, the Biometric Commissioner, that he, without official remittance, conducted his own investigations into the issue and reported in his 2014 Annual Report[141] that, without any public or Parliamentary consultation whatsoever, he understood that some twelve million custody images had been uploaded onto a live, searchable system in March 2014.[142]

He was sufficiently alarmed by developments that he began raising concerns with the Information Commissioner, chief police officers and the Home Office. His especial concern was that the new police database included images of 'hundreds of thousands of individuals who had never been charged with, let alone convicted of, an offence' and that 'more are being loaded to it each day'.[143] This was 'notwithstanding the fact that, in light of judgment in *RMC*, it seems likely that many of these images should no longer be held by the police'.[144] In order to protect civil liberties, he concluded that 'urgent steps should now be taken to ensure that they [custody images] be governed by an appropriate regulatory regime'.[145]

---

[138] See, for example, T. Whitehead, 'Police breach human rights by keeping photos of innocent' *The Telegrap*h (London, 22 June 2012) and J. Meikle, 'Police may have to destroy photos of innocent people after court ruling' *The Guardian* (London, 22 June 2012)
[139] Above n.120 [58]
[140] College of Policing, 'Management of Police Information' (3rd edn, 24 October 2014)
[141] A. MacGregor, 'Commissioner for the retention and use of Biometric Material – Annual Report 2014' (The Office of the Biometric Commissioner, November 2014)
[142] Ibid, 103
[143] Ibid, 105
[144] Ibid
[145] Ibid, 106

The Biometric Commissioner was sufficiently concerned by what he found that he felt compelled to enter his reservations into evidence before a Commons Science and Technology Committee convened in the autumn of 2014 to review the use of biometric data and technologies.[146] When asked to address the Biometric Commissioner's concerns and inform the committee about the searchable PND database, Chief Constable Chris Sims, giving evidence on behalf of ACPO, claimed that he was 'not aware of force use of facial image software at the moment'.[147] The Biometric Commissioner described this evidence as 'surprising',[148] before Sims attempted to qualify his statement by stating that facial recognition was 'not my area of speciality'.[149]

The Committee were sufficiently confused by the apparent lack of understanding of police data systems by the chief officer sent by ACPO to provide evidence to them about precisely that issue that they asked the Home Office directly to clarify matters. Contrary to Sims' claims, they confirmed that they knew the police were considering a facial recognition system in 2012 and 'that functionality was made available to all PND users' (i.e. all police forces in England and Wales were able to use it) on 28 March 2014'.[150] Quite whether Sims was genuinely mistaken or was attempting to obfuscate matters is not clear. What is clear is that he entirely misrepresented the police position on the retention, storage and use of custody images, many tens of thousands (at least) of which, by this time, the police had been unlawfully retaining for some thirty months.

The Committee noted that 'two and half years later [since the judgment in *RMC*] and still no updated policy [on retention of custody images] has been published'.[151] The committee was therefore 'dismayed to learn that, in the known absence of an appropriate governing framework, the police have persisted in uploading custody photographs to the PND to which facial recognition software has been applied'.[152] The Committee recommended that statutory oversight to the use of custody photographs be added to the remit of the Biometrics Commissioner.[153]

---

[146] Science and Technology Committee, *Current and future use of biometric data and technologies* (HC 734, 2014 – 15 6 – I)
[147] Ibid, 31
[148] Ibid, 32
[149] Ibid, para.96
[150] Ibid, 'Written evidence submitted by the Home Office' (BIO0038 January 2015)
[151] Ibid, para.98
[152] Ibid, 33
[153] Ibid, para.105

When pressed about the apparent procrastination on the part of the Home Office in rectifying the legislative defects highlighted in the *RMC* case, Lord Bates told the Committee that the Home Office was instituting a 'policy review' into the matter which would involve a consultation of 'key stakeholders'.[154] That review took two years and a report was finally published in February 2017.[155] This contained, almost five years after the decision in *RMC*, an amended and detailed policy for the retention of custody images which is now fully incorporated into the 2014 MOPI Guidance[156]

The provisions are complex. In broad terms, there is now a 'presumption in favour of deletion' for custody images taken of individuals who are ultimately not convicted of an offence. However, such images are not automatically deleted, but rather eligible data subjects may make an application for deletion at the conclusion of the proceedings against them.[157] The police may discretionarily refuse the application for deletion, but they must justify that decision where a risk assessment shows a continuing 'substantial risk of harm', where evidence shows the individual may be 'dangerous' (such as entry on the Violent or Sexual Offenders Register), where an active investigation against the individual is ongoing, where the individual has known links of organised crime or terrorism or where there is a need to enforce a civil order.[158] As the vast majority of suspects are likely to fall outwith those parameters, it is submitted that these provisions should enable the majority of unconvicted persons to have their custody image(s) deleted (if they apply to do so).

For those convicted of an offence, different rules are applicable. There exists a presumption in favour of deletion for those convicted of a non-recordable offence, but only after six years have passed since the conviction. Where no request for deletion is made, a review of the image, with a presumption that the image will be deleted, should take place after six years and every five 'clear' years after the first review (if the image is to be retained). Retention must only be justified on the same grounds as those for unconvicted individuals[159]

---

[154] Ibid, Oral Evidence, Q.152
[155] Home Office, 'Review of the use and retention of Custody Images' (February 2017)
[156] Above n.140 at 'Information Management, Retention, Review and Disposal', Ch. 1.1 'Custody Images'. Doubtless intending to prevent repetition of the judicial criticisms that their guidance on data collation and retention was not easily ascertainable, the NPCC now publish the most up-to-date editions of the MOPI Guidance online and in full at <https://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#accepting-a-request-for-deletion> accessed 26 March 2019
[157] Above n.155, 9, paras. 2.3 – 2.4
[158] Ibid, para. 2.4
[159] Ibid, 11, para.2.14

However, where an individual is convicted of a recordable offence, there is no presumption in favour of deletion.[160] Those convicted of a 'Group 3' offence[161] must also wait for six years before applying for image deletion. Those convicted of 'Group 1' or 'Group 2' offences must wait ten years from conviction (or release from custody, if a custodial sentence was passed). If no application is made a police review should take place after the same time periods, but without a presumption in favour of deletion[162]. A new review, or application for deletion, can only be made after the passing of five 'clear' years (for Group 3 offences) or ten 'clear' years (for Group 1 and 2 offences).[163]

Different rules apply to juveniles. Applications made to delete images taken of juveniles who are not convicted are subjected to a 'strong presumption in favour of deletion' at the conclusion of proceedings against them.[164] The same exceptions apply as to adult suspects, except that the risk of harm must be '**very** [original emphasis] substantial', rather than 'substantial'.[165] However, where no application to delete is made, then the image will be retained and reviewed after the same 'clear' periods as for adult offenders, depending on the 'Group' of the alleged offence,[166] albeit that there will be a strong presumption in favour of deletion at that review.[167] The same rules apply in respect of juveniles convicted of an offence save that there is a presumption in favour of deletion at the first review stage for recordable offences[168] and a strong presumption in favour of deletion for non-recordable offences.[169]

Although a full critical evaluation of the updated policy regarding custody images falls largely outwith the scope of this research, some general comments ought to be made. The review, and the implementation of the recommendations within it, has been widely criticised in a number of respects. The failure to implement legislation similar to that for the BCD regime was justified by reference, among other things, to the ready availability

[160] Ibid, para 2.11
[161] These are the same as the original 'Category 3' offences in the 2005 MOPI Guidance. 'Category 1' and 'Category 2' offences are also synonymous with their new 'Group' counterparts. See above n.156, ch.2.3.3
[162] Above n.160
[163] Above n.155, 11, para.2.12
[164] Ibid, 12, para.2.16 – 2.17
[165] Ibid, para.2.17
[166] Ibid, 13, para.2.19
[167] Ibid, para.2.20
[168] Ibid 14, para.2.23
[169] Ibid, para.2.25

of facial imagery in general and on social media, and the diminishing usefulness of photographs over time.[170] This, it is submitted, is rather spurious. There is a marked difference between people consenting to using their own image on Facebook or Twitter (notwithstanding the millions of people who chose not to do so) and the statutory imposition of providing an image to the police to be stored on a central police database for a period of years. Moreover, it is difficult to understand why the diminishing of usefulness over time of a photographic image (as compared to BCD, particularly) should lend itself to a lengthier retention period, rather than a shorter one; if the data becomes less and less useful, it is submitted that the justification for retaining it must become lesser, not greater.

The new proposals considered, and rejected, creating an automatic deletion process (as happens for BCD) largely on grounds of 'cost to the taxpayer'.[171] Quite how the new proposals are more cost effective, considering that each application for deletion will be manually handled, is not clear; a point reinforced by the Biometric Commissioner in his response to the review.[172] The Biometric Commissioner was unimpressed generally by the review, noting among other reservations that in their refusal to extend his remit to the use of custody photographs (though this is still being 'considered')[173] the Home Office had left 'the governance and decision making of this new process entirely in the hands of the police'[174] and claiming that the discretion afforded to chief officers might result in decisions to delete images amounting to a 'postcode lottery'.[175]

The Home Office's own Biometrics and Forensics Ethics Group were not much more supportive. At the written invitation of the Home Office, the Group were asked to respond to the review. They provided that they too could not support the view that facial images were less intrusive than other biometric data, that they were 'disappointed' at the absence of a public consultation prior to the review' (in spite of Home Office assurances made to the Science Committee that 'key stakeholders' would be consulted. Presumably the Home Office 'consulted' with the police and not many others besides) and recommended that a system should be built with automatic deletion capability. The latter was especially

[170] Ibid, 15, para.3.7
[171] Ibid, 3, para.1.13
[172] P. Wiles, 'Response to the Home Office review of the retention and use of custody images' (17 March 2017)
[173] Above n.155, 18, para.3.24
[174] Above n.172
[175] Ibid

important because the Home Office, presumably by design, had 'not publicised the new retention regime and it was likely that there was a general lack of public awareness of it'.[176]

This, it is submitted, is perhaps the most critical failure in the new regime; the need for individuals to apply for deletion, rather than mirroring the BCD system where data is automatically deleted after the applicable qualifying criteria are met. This means that, in actuality, hundreds of thousands of unconvicted people almost certainly still have custody images retained in police records, particularly after the Home Office's promised 'publicity campaign'[177] amounted to practically nought. This point was made by Baroness Jones, who asked in a House of Lords debate on the review: 'surely it would be easier for the police to just delete those innocent people without putting them to the trouble of applying'?[178]

If the database still holds countless images of unconvicted individuals, it is difficult to reconcile it with the judgment in the *RMC* case. It is, therefore, submitted that even the updated regime is likely to be unlawful and subject to successful challenge if (or when) such a challenge is brought. That is the view of the Biometric Commissioner[179] and it is the view of the Science and Technology Committee, who returned in 2018 to the issue of custody image retention and scathingly concluded that:

> The Government's approach is unacceptable because unconvicted individuals may not know that they can apply for their images to be deleted, and because those whose image has been taken should not have less protection than those whose DNA or fingerprints have been taken.
>
> The Government must ensure that its planned IT upgrade under the Home Office Biometrics Programme is delivered without delay, and is used to introduce a fully automatic image deletion system for those who are not convicted. If there is any delay in introducing such a system, the Government should move to introduce a manually-processed comprehensive deletion system as a matter of urgency.

[176] Biometric and Forensic Ethics Group, 'Response to the Home Office custody images review' (25 August 2017)
[177] HL Deb 2 March 2017, vol.779, col. 947
[178] Ibid, col.948
[179] Above n.172

> [They] should also set out the Home Office's assessment of the lawfulness of its deletion-on-application response to the 'RMC' case, and the legal advice underpinning that assessment.[180]

This author respectfully concurs with that position in its entirety and cannot add anything meaningful further to it.

9.7 Conclusions

In many respects, this research has now 'turned full-circle'. As has been shown, the police have collected various criminality datasets for almost two centuries. Although today these are stored in separate repositories and used for slightly different purposes, the central tenet which governs each is that they are used as a conjoined means of detecting and preventing crime and apprehending offenders. It is not correct to see them as separate entities in their own right. Indeed, and as has always been so far as the police are concerned: 'the fingerprints, DNA and PNC record are treated as an integrated whole'.[181]

This is why developments in the legislative and jurisprudence regarding each of these datasets has a direct relevance and applicability to the others. What emerges is a clear pattern in almost all areas. For a very long time, the police were given an unfettered discretion to collate, store and retain whatever data they saw fit. The judiciary seemed reluctant to impose upon that discretion while Parliament, and more specifically the Home Office, have actively supported and facilitated it. This state of affairs survived even through the creation of PACE, was accelerated in the legislative developments immediately after the terrorist attacks on September 11 2001 and was latterly bulwarked by the findings into the *Soham* murders in 2003.

The decision in the *Five Constables* case may, in time, come to be seen as the high-watermark of that approach and change is coming from without, rather than within. While those with a vested interested in expanded data collection, storage and retention (the police and the Government, particularly) remain predictably resistant to changing the parameters (except to expand them, where possible), they are nonetheless shifting towards a more regimented retention process driven predominantly by European, rather

[180] Science and Technology Committee, *Biometrics strategy and forensics services* (HC 800, 2017 – 19, 5 – I) [44] [45]
[181] Per Commander Gibson in evidence to the court in *RMC*, above n.120 [22]

than domestic, jurisprudence. Unconstrained by the traditional deference afforded to the police by Parliament and the English judiciary, the European Court of Human Rights is casting an increasingly critical eye on both the data retention practices of the police and the legislative provisions which facilitate them. Their scathing dismissal of the House of Lords' judgment in *S and Marper* led to a complete legislative overhaul to the law governing biometric criminality data and significant limitations being placed upon the police, particularly as regards juveniles and those who are not convicted of offences.

Domestically, the English judiciary, despite some missteps (such as that in *Gaughran*), have consequently developed a hitherto critical attitude towards police attitudes on, and general handling of, criminality data, and adverse judgments are now being handed down. The most significant of these domestically has resulted in the centuries old practice of collating and storing custody images being declared unlawful and a new (albeit limited) regime being implemented regarding these, restricting the police capacity to retain these. This regime is especially protective of juveniles and those who are not convicted of offences.

Of the three main bulwarks of police criminality data collections, then, only the PHOENIX collection now remains untouched. This is despite the decision in *MM*, which expressly dealt with an identical collection in Northern Ireland (and the same retention regime as that in England and Wales), and which the judiciary have so far managed to avoid addressing by restricting their application of the principles contained in that judgment only to the 'unconvicted'. That is an approach rejected by many in the academic community and which this author finds no express support for in the decision of *MM* itself; a case which dealt with a caution record, no less. If, as this author anticipates, the ECtHR finds error in that approach when making a decision in the *Gaughran* appeal, the English jurisprudence will likely become untenable and a renewed litigation attack on the PHOENIX retention regime will be inevitable, unless Parliament acts to prevent it.

Even if it does not, then it is difficult to reconcile the present position so far as PHOENIX is concerned. If the 'unconvicted' do not deserve to have their BCD held once proceedings against them conclude, or their custody image held likewise, how can it be justiciable to hold their data on PHOENIX until they reach age 100 years? A similar critical comparison may be made in respect of juvenile offenders and those juveniles issued reprimands and warnings. The regime for PHOENIX data is now so much more intrusive as regards the

length of retention of data as compared to its bedfellows that legitimate questions as to why this is so now need to be addressed.

Quite simply, as was acknowledged by Commander Gibson in RMC. 'If the DNA and fingerprints continue to be retained, then so too should the PNC data'.[182] That is a sensible proposition. But the question which requires consideration now is: if the DNA and fingerprints have been destroyed, then why should not the PNC data be too?

[182] Ibid

10
Summary of research findings and recommendations

10.1 Introduction

This research set out to answer four research questions. It is submitted that each of them has been answered. It is not intended for this chapter to regurgitate earlier findings, but instead to consolidate the answers that have been revealed and, where possible, to make recommendations for the future concurrent to these. Each of the research questions will be dealt with in the chronological order provided in the opening chapter of this research.

10.2 Answering the first research question

The 'traditional' definition of 'criminal record' takes the noun version of the word 'criminal'; 'to be convicted of a crime'.[1] It was hypothesised at the outset of this research that this 'traditional' view that a 'criminal record' consisting simply of a list of court convictions against a named individual would not be borne out. It is submitted that this hypothesis has been shown to be correct.

In reaching that conclusion, particular trends can be evinced. As chapter two of this research shows, the embryonic collections of criminality data which emerged in the middle of the eighteenth century were not built by statutory mandate, nor constrained by legislative boundaries. They were collections built by individuals with an involution in the criminal justice system; magistrates, local policing groups, prison governors and the like. These individuals clearly saw merit in collating criminal convictions but only as part of a wider collection of other criminality data which might potentially assist them in their duties; warrants for arrest, allegations of crime, suspicious activity, photographs and 'distinctive marks' were also just some of the data recorded against named individuals.

The first legislative mandate for the collection of 'criminal records' imposed an obligation on police to make a 'register of those convicted of an offence'.[2] Parliament, it seems, was only interested in knowing about those who committed crimes and in doing so instituted, literally, a record of convicted criminals; a 'criminal record'. The repeal of that provision

[1] B. A. Garner, *Black's Law Dictionary* (9th edn, Thompson Reuters 2009) 430
[2] See ch.2.4 of this research

and replacement in 1871 with a more limited requirement to record only those convicted of two or more offences did not change the fundamental tenet of the Parliamentary constraint, which was that the central 'record' simply list those who had been convicted of a crime (or more than one, in the strict prescribed legislative form) and that a photograph of each listed person be attached so that the correct record be matched to the correct individual.

This, it is submitted, forms the basis for the traditional view of 'criminal records'. The traditional view that a criminal record is a list of court convictions listed against an individual must stem from the legislative requirements which instituted a register on precisely those grounds. That traditional definition certainly has a deep-rooted core; the legislative mandate for the collection of a central 'criminal record' lasted for ninety-eight years.[3]

However, what also clearly emerges is that the police, taking their lead from the early criminality data collators, were contributing to this centralised 'criminal record' but were also simultaneously collecting their own vast repository of criminality data, independent of any statutory obligation to do so; criminal convictions, arrest details, warrants, fingerprints and *modii operandi* were just some of the reams of personal data relating to known and suspected offenders being stored by the developing police forces in England and Wales.

Not only were the police not obligated to make such a collection, but they were also, conversely and concurrently, not constrained by any legislation from making such an extensive collection of data. Such lack of constraint largely stemmed from the underlying principles which had birthed those early police forces; the largely permissive legislation which allowed, but did not mandate, the creation of local (rather than a single centralised) police forces,[4] the notion of 'policing by consent', rather than by overt force,[5] and the establishment by the turn of the twentieth century of almost complete autonomy of chief constables, who by that time were constrained neither by the public nor local or central

[3] The Habitual Criminals Act 1969 first instituted the register on these terms, and it was only in 1967, with the implementation of the Criminal Law Act 1967, that the amended requirements of the Prevention of Crimes Act 1871 were repealed.
[4] See predominantly the Municipal Corporations Act 1835 and the County and Borough Police Act 1856. For a thorough examination of both, see D. Taylor, *The New Police in Nineteenth Century England: Crime, Conflict and Control* (Manchester University Press 1997) 12 – 43
[5] J. Jackson et al, *Just Authority? Trust in the Police in England and Wales* (Routledge 2013) 7 – 9

government, save where legislation expressly provided as such.[6] Indeed, by the turn of the twentieth century and the opening of the National CRO, the police had become 'an important and significant influence on their own development and this influence grew as the police surrounded themselves in mystique and began to be accepted as experts on questions of crime and order'.[7]

Independent of either obligation or constraint, the police therefore built their own extensive repository of criminality data. These records were far more expansive than the centralised 'criminal records' kept by the Metropolitan Police under their statutory imposition related to monitoring habitual offenders. They were an attempt to build a comprehensive police intelligence repository, purportedly useful in the investigation of crime and suspected offenders. These, it is submitted, were the 'police records' to which Uglow referred.[8]

This research indicates that these separate, but interlinked, collections, continued to be expanded into the middle of the twentieth century. The statutory 'criminal records' register continued to be compiled at the National CRO under the Metropolitan Police and the 'police records' were greatly expanded, both by individual forces and in considerable depth at the various 'clearing houses' and Regional CROs which opened in the middle of the twentieth century.

In 1967, the statutory obligation to maintain a register of criminal convictions was repealed. However, as has been shown, the police (or, more accurately, police officers at the various CROs) simply continued to collate, store and retain a vast repository of criminality data, independent entirely of any statutory obligation to do so. The register of criminal convictions was not deleted or even discontinued – it was instead simply subsumed into the CRO data collection exercise. This, it is submitted, is the point at which the demarcation between 'criminal records' and 'police records' ceased to exist, both in a legal and a practical sense. In 1967, the 'police records' became the 'criminal records'.

This process was accelerated when the PNC gave the police the opportunity to store all of their criminality data in electronic form, including all criminal conviction data and their 'supplementary data'; arrests, warrants, descriptions, *modii operandi*, police markers and

[6] M. Brogden, *The Police: Autonomy and Consent* (Academic Press Inc. 1984) 39 – 73
[7] C. Emsley, *The English Police: A Political and Social History* (Routledge 2014) 5
[8] See ch.1.2 of this research.

all of the other data which now must properly be considered part of the 'criminal record'. The implementation of the permissive provisions of s.27(4) of PACE did little more than close a legal lacuna which might have arisen out of the DPA 1984; the police had never stopped collecting conviction data and were still recording it centrally at the NIB in preparation for uploading to the PNC one year later. The entire circle turned when PHOENIX became operational in 1995; the former 'police records' became the central repository of criminal data for all police forces in England and Wales. For police officers today, there must be no demarcation whatsoever between a 'police record' and a 'criminal record'. They are simply different screens of data on the same computer application. PHOENIX, it is further submitted, *is* the 'criminal record' and the nominal listings within it *are* the 'criminal records'.

If further proof were required that PHOENIX nominal listings are now properly considered the 'criminal records', then one need only look at what the process is involved in the production of certificates after a 'criminal record check'; indeed, of the three types of 'criminal record' check permissible by statute,[9] only the 'basic' check will return a certificate concurrent with the 'traditional' view of criminal records.

The standard' check, meanwhile, will provide details of reprimands, cautions and warnings. These are not 'court convictions'[10] in that they are neither disposals made in court, nor are they 'convictions',[11] but they are nonetheless stored in the central records and disclosed on the standard check. In any practical or legal sense of the word, these must also now be rightly considered as part of an individual's 'criminal record. The discretionary element of the enhanced check, meanwhile, potentially allows the for the inclusion of information contained within the 'event history' section of PHOENIX; arrests, warrants, PNfDs and acquittals are all routinely included on this type of 'criminal record' check.[12]

[9] See chapter 8.5 of this research.
[10] Despite the rather feeble attempt by the Government to make them so, by amending s.27(4) of PACE to include them as 'convictions' for the purpose of retaining criminal record data (inserted by s.85 of the Protection of Freedoms Act 2012). The retrospective inclusion of warnings and reprimands, which were expressly confirmed to not be convictions by successive Home Office guidance, is particularly questionable.
[11] See chapter 4.4 of this research.
[12] See chapter 8.5 of this research.

For the purposes of a 'criminal record' check, therefore, potentially any of the information included in PHOENIX might be disclosed, depending on the check being requested. For the vast majority of the four million or so citizens who receive a criminal record certificate from the DBS each year,[13] their 'criminal record' is not a simple review of their court convictions. It is a check of their entire PHOENIX nominal listing.

Recommendation 1

In order to resolve the pervasive confusion as to what constitutes a 'criminal record', a new, statutory definition of 'criminal record' should be provided which accurately reflects the records that are being collated, stored and retained on PHOENIX and which might be used for the purposes designated of them.

Interestingly, in the Data Protection Act 2018[14], 'personal data relating to criminal convictions and offences' is defined as:

> Personal data relating to the alleged commission of offences by the data subject[15] or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing'.[16]

This, it is submitted, is a much better definition of 'criminal record' than any other extant statutory attempt to define one, in that first part encompasses information held in the 'event history of PHOENIX' and the second encompasses all cautions, reprimands, warnings and convictions. If, in meeting this recommendation, Parliament elects to try and utilise an extant statutory provision, it is submitted that this is perhaps the best present example suitable for adaptation.

Recommendation 1(a)

On this basis, it is supplementarily recommended that the definition provided by s.11(2)(b) of the Data Protection Act 2018 either be the definition of criminal records to which all other applicable legislation now be directed or, alternatively, be the basis for a slightly

[13] In 2017/18, over three and a half million of the four and a half million checks carried out were 'enhanced' checks. That pattern was repeated in each of the two preceding years; see Disclosure and Barring Service, 'Annual Reports and Accounts for the period 1 April 2017 to 31 March 2018', (HC 1367, 19 July 2018) 8
[14] 2018, c.12
[15] S.11(2)(a) of the Data Protection Act 2018
[16] Ibid, s.11(2)(b)

reworded version to include reference to PHOENIX and the specific categories of data contained within it.

10.3 Answering the second and third research questions

It was hypothesised at the outset of this research that the thesis would likely show that that the police did not comply with all of their obligations pursuant to the various Data Principles outlined in the Data Protection Act 1984 and the Data Protection Act 1998.

It is submitted that the research has confirmed both hypotheses. In chapter five, it was shown that the concern of unlawful access to the PHOENIX data identified as early as the 1970s by James Rule persisted throughout the following decades.[17] Despite a relative reduction in press attention, the problem has not been fully eradicated; a 'Freedom of Information Request' to Gloucestershire Constabulary in 2017, for example, showed that five officers and support staff were found to have unlawfully accessed PNC data between 2014–17,[18] while a further 'Freedom of Information Request' to the British Transport Police showed that, in the same period, they had investigated two instances of unlawful staff access to the PNC. These resulted in a caution being issued to one individual and a successful prosecution against the other.[19] A Home Affairs Committee reporting in July 2012, meanwhile, found that there still existed a 'close inter-marriage' between investigators and the police, which represented a 'significant risk'.[20] The Committee found copious evidence that investigators were paying officers for access to police data and concluded that there existed 'an unacknowledged but deep-rooted intertwining of a private and unregulated industry with our police forces'.[21]

These reoccurrences suggest strongly that the problem is persistent and that additional measures are required to ensure data protection compliance. They also, it is submitted, suggest that there is a police tolerance of such unlawful access, so long as the issue is

[17] See ch.5.5 and ch.6.5 of this research.
[18] Gloucestershire Police, 'FOI Request. Officers and Staff illegally accessing PNC' (*Gloucestershire Constabulary*, 9 February 2017) <https://www.gloucestershire.police.uk/more-on-us/freedom-of-information/disclosure-log/operational-policing/officers-and-staff-illegally-accessing-pnc/> accessed 29 May 2019
[19] British Transport Police, 'Illegal access to the PNC' (Request 0051 – 17, *British Transport Police Online Log* February 2017) <http://www.btp.police.uk/about_us/your_right_to_information/publication_scheme/disclosure_log/complaints_and_discipline.aspx> accessed 26 April 2019
[20] Home Affairs Committee, *Private Investigators* (HC 100 2012 – 13, 4 – I) 11, para.27
[21] Ibid, 12

one of 'access', rather than unlawful 'use'. This was postulated by Lister and Rowe, who believe that there is sufficient evidence to suggest that 'this is particularly so where access is motivated by professional curiosity, rather than malicious intent or nefarious motives…the idea that police members are *entitled* [original emphasis] to access information may be culturally ingrained within police forces'.[22] Not only, therefore, is there a lengthy history of breaches in this regard, but there appears little prospect of them being prevented in future.

It is clear, according to this research, that unlawful access to the PHOENIX data continues, that it may even be tolerated by certain officers or forces and that whatever measures are in place to prevent this, that these are insufficiently robust to eliminate them. The responsibility for preventing this lies with the data controller/processor; i.e. Chief Officers. It is submitted that the failure of the Commissioner to issue Enforcement Notices against Chief Officers at all,[23] and particularly when the most egregious examples of unlawful access emerged, has discouraged Chief Officers from taking a more proactive, preventative approach to the problem.

Recommendation 2

It is, therefore, recommended that the Information Commissioner take a far more pro-active approach to instances of unlawful access to PHOENIX data. Enforcement action should be considered whenever appropriate and Enforcement Notices should be issued to deal with particularly egregious examples. This will encourage better practice among forces in preventing unlawful access, and should decrease the number of data breaches.

The problem of the data quality,[24] on the other hand, appears to have been resolved. The Home Office certainly thinks so: a recent Home Office assessment claimed that the 'PNC currently has a good data quality regime and this should be maintained…'[25] This is achieved, say the Home Office, by a combination of data input predominantly by a specially trained team of central administrative staff[26] and by a process of periodic internal auditing by police data processors.[27]

[22] S. Lister and M. Rowe, *Accountability of Policing* (Routledge 2016) 94
[23] See chapter 6.5 of this research.
[24] See chapter 5.4 and 6.4 of this research
[25] Home Office, 'National Law Enforcement Data Programme: Law Enforcement Data Service – Privacy Impact Assessment Report' (July 2018) 25
[26] Ibid, 13
[27] Ibid

It is submitted that these assurances ought not to be taken at face value and that questions must remain as to the quality of the PHOENIX data. One reason for this is that, as this research has shown,[28] the police hardly have an enviable record of ensuring good data quality when left to their own devices. If the picture is as rosy as the Home Office suggest, then it only is so because the police were inspected, repeatedly, to ensure that their house was put into sufficiently good order. Another reason for doubt is that the 'auditing' process appears to be entirely internal, and wholly opaque. None of these audits appear in the public domain and therefore are not subject to external scrutiny.

Another, and perhaps the most persuasive, reason for casting some doubt as to the veracity of these claims, is that the quality of the data on the PND – the 'other' principal police database for which police forces are responsible for data collation and management and for which chief officers are responsible as processors – is almost as parlous as the data once was so publicly found on the PNC.

It is not necessary as part of this research to conduct detailed research into the data quality of the PND, but some general comments will be made. The implementation of mobile data terminals, as a means of inputting data onto local systems which would then be added to the PND, has exacerbated some of the pre-existing problems as to the quality of data but Lindsey et al had suggested that the implementation of the PND in 2010 might 'place additional pressure and serve as a key driver for ensuring good data quality'.[29] It did not. HMIC, conducting an inquiry into the intelligence failings into the investigation of Jimmy Saville, found a significant variance between forces and their respective timeliness of inputting data to the PND,[30] so that the availability of data on the PND information relating to suspect depended largely on which police force had dealt with the suspect.[31] Moreover, 'accurate and comprehensive information…remains elusive'.[32] Quite simply, the applicable MOPI guidance on police data systems 'is not being given full effect in all forces'.[33]

---

[28] See chapter 6.4 of this research.
[29] R. Lindsay, T. Jackson and L. Cooke, 'Mobile access to information systems in Law Enforcement: An Evaluation of its implications for Data Quality' (2010) 13(2) The Electronic Journal of Information Systems Evaluation143
[30] Her Majesty's Inspectorate of Constabulary, 'Mistakes were made: HMIC's review into allegations and intelligence material concerning Jimmy Saville between 1964 and 2012' (London, March 2013) 34
[31] Ibid, 35
[32] Ibid
[33] Ibid

As recently as 2018, the Home Office lamented that, as regards the PND, 'data quality and consistency are important parts of privacy…and poor data quality is a barrier to this. Data which is incomplete, inconsistent, not meaningful or misinterpreted can lead to poor decisions, wasted time or missed opportunities'.[34] Work to 'encourage forces to achieve the highest possible standards in this area is continuing' and there are proposals to introduce national data standards to try and bring up the quality of the data.[35]

There is an almost depressingly familiar tenor to the criticisms regarding data quality for the PND; lack of timeliness, inconsistent input, the need for HMIC inspections and a variety of other, not insignificant criticisms all form part of the ignoble history of PHOENIX data quality. It appears that the proverbial leopard has not changed its spots, so far as the attitude to data quality is concerned. It is, therefore, extremely difficult to accept at face value the claims that the PNC data is quite as in order as the Home Office and the police claim it to be, and a degree of healthy scepticism must be exercised.

Recommendation 3

It is recommended that an external organisation be charged with conducting periodic inspections of the PHOENIX data to ensure that data quality is of a suitably high standard, measured against the Data Principle requirements of relevancy, adequacy,[36] accuracy and currency.[37] These will improve police operational efficiency.

Previous inspections by HMIC have helped to drive and maintain improved data quality, and it is further recommended that HMICFRS (as they are now) conduct these inspections. Reports should be released into the public domain, to ensure transparency and increase public confidence in the police data collection processes. The Information Commissioner should be included on the circulation list of these reports and where these indicate that police data collections are of insufficient quality, Enforcement action should be considered to ensure Data Protection compliance.

This research has also found that the police are making unlawful arrests. These are extremely difficult to quantify but these are nonetheless occurring and the resultant arrest

[34] Above n.25, 14
[35] Ibid
[36] Per s.37 of the Data Protection Act 2018.
[37] Per s.38(1) of the Data Protection Act 2018.

data is being included in criminal records. Examples highlighted by this research include the common police practice of arresting those who attend the police station voluntarily to assist in police investigations and people who have been arrested without lawful justification under s.24 of PACE. The former should not be ordinarily arrested until or unless sufficient evidence emerges to justify that arrest under s.24 PACE or a warrant is obtained, while the latter is demonstrably unlawful under the applicable statute. In both cases, arrest data is retained in the 'Event History' section of the Nominal Record on PHOENIX.[38]

Recommendation 4

It is recommended that the NPCC provide detailed guidance to all police officers as to the appropriate means of dealing with volunteers. Where such an individual is arrested, it is recommended that arrest data not be added to the 'Event History' section of PHOENIX unless that arrest results in a charge being issued. Any arrest data currently being held on PHOENIX relating to volunteers who were not subsequently charged, or any such data collated contrary to this recommendation in future, should be pro-actively deleted. If such 'arrest-only' data is to be retained instead on the PND, that data should be reviewed in accordance with MOPI guidance to ensure its retention continues to be compliant with the applicable Data Principles.

It is also evident from this research that there are legitimate concerns regarding the issuing of cautions. Some individuals accept cautions because they believe, erroneously, that are an 'easy option' which allow them to go home without further adverse consequences, while others are effectively induced into accepting them after investigating officers intimate that a confession may result in a caution being issued, rather than a prosecution being brought.[39]

The issue is compounded by the nature of cautions; they are intended for first-time, minor and usually juvenile offenders.[40] Such individuals will often be unrepresented at the police station and have little knowledge or experience of the police investigatory process. Many will be in a heightened emotional state when deciding whether or not to make a confession in the 'hope' of being cautioned.[41]

[38] See chapter 6.3.1 of this research.
[39] See chapter 6.3.2 of this research.
[40] See chapter 4.4.3 of this research.
[41] Above n.39

The Ministry of Justice issued formal guidance on the issuing of 'simple cautions' in 2015.[42] It was intended to replace all previous guidance and provides that it **must** [original emphasis] be applied to all decisions relating to simple cautions.[43] It provides detailed guidance on the administration of simple cautions, including the provision of a 'simple caution form' which the offender should sign and which is 'a form setting out the implications of the simple caution'.[44] A template or other exemplar is not provided, but it is stated that the form must include information which informs the recipient that they have admitted an offence[45] and that the admission and caution will form part of the individual's criminal record[46] which may be used in future legal proceedings[47] or disclosed via a DBS criminal record check.[48] The form should also inform the suspect that: 'the caution will be retained on the PNC. ACPO guidelines set out how long this information should be retained for'.[49]

The introduction of a 'simple caution form' is welcome but difficulties persist. Although the offender should be informed before signing that they are entitled to take legal advice,[50] this is likely to be limited to either telephone advice or advice from a duty solicitor, where either is available. Where a delay in access to either occurs, a suspect may elect not to take legal advice in the hope of 'going home' more expediently. Moreover, many suspects do not utilise their right to legal advice at the station, and so will sign without receiving this.

Additionally, it is not clear why an exemplar form cannot be provided, so that there is a consistency among forces and to ensure best practice. Poorly drafted forms may cause confusion among those to whom the form is intended to be issued and give rise to subsequent judicial challenge. It is not difficult to envisage a potential challenge where the form includes unnecessarily technical or legal language – the reference on a form to 'ACPO guidelines', and even 'the PNC', will mean little to the non-expert reader. Moreover, it is submitted that such terms do not properly outline the full implications of the retention of the caution. Indeed, they may even (unintentionally or otherwise) obfuscate those

[42] Ministry of Justice, 'Simple Cautions for Adult Offenders' (13 April 2015)
[43] Ibid, 3
[44] Ibid, 17, para.80
[45] Ibid, 14, para.63
[46] Ibid, para.64
[47] Ibid
[48] Ibid, 15, para.65
[49] Ibid, para.66
[50] Ibid, 16, para 78

important ramifications; the currently guidelines set the retention period as being until the suspect reaches age 100 years or being deceased. In essence, the caution will be retained for the life of the data subject, even though it will become 'spent' as soon as it is issued. This is critical information which needs to be expressed clearly to the intended recipient prior to the imposition of the caution.

Recommendation 5

The Ministry of Justice should draft, and circulate, an 'exemplar' simple caution form to be used by all forces for use in the administration of all simple cautions. This should include all of the baseline information intimated in the official guidance but should be drafted in plain English to ensure that those who sign the form understand fully the ramifications of the caution.

In particular, the caution form should avoid reference to 'ACPO Guidelines' and instead make clear that the caution will be retained until the suspect is aged 100 years and, subject to the 'protected caution' regime and the ROA 1974, is liable for disclosure if the individual applies for a subsequent criminal record check.

The form should also explicitly advise an individual to take independent legal advice before signing it, and make provision for the individual to explain, in writing, why they have not received this if they do not.

This will reduce the number of individuals who are unlawfully, or 'illegitimately' cautioned and, by ensuring that a higher number of individuals who receive cautions have actually committed offences, offer greater opportunity to police forces to utilise the data more effectively for their operational purposes.

10.4 Answering the fourth research question

It was hypothesised that the approach taken in the *Five Constables* case, which afforded an almost complete operational discretion to the police in determining how long their criminal record data is to be retained is flawed in several respects. It is submitted that this research has illustrated, at least, that there are considerable doubts as to the necessity of the policy *in situ*.

This research has demonstrated that criminal record data was originally collated because the earliest protagonists believed that doing so would enable them to prevent and better investigate criminal behaviour.[51] Such a position found favour over the next century or so as statistical evidence emerged to show that large volumes of crime were committed by small numbers of recidivistic offenders.[52]

However, what this research further shows is that the police do not appear to have utilised this knowledge to operational effect, other than by collating a huge mass of criminal records data. Although well-supported in criminological theory, attempts to envoke 'intelligence-led policing' largely failed in practice[53] and the question which remains entirely unresolved, even after over a century of extensive criminal record data by the police, is how the knowledge that a small number of highly active recidivists commit disproportionately voluminous offences has actually translated into police operational processes which prevent, or investigate, crime more effectively.

Indeed, what this research has shown is that, if anything, many forces have largely desisted from engaging in any analytical or pro-active forms of policing,[54] instead preferring to rely on 'local knowledge', 'experience' and reactive investigation techniques which often amount to little more than responding to a reported crime by identifying a pool of 'usual suspects' and interrogating these to see if this will 'get results'.[55]

Indeed, some forces recently simply eschewed criminal investigations into serious offences in favour of picking 'low-hanging fruit' in order to meet disposals targets and 'get results'. For example, an HMIC investigation[56] in 2013 found that Kent Constabulary had deliberately prioritised 'clear-up' targets over other policing concerns, incorrectly recording reported rapes as 'no-crimes'[57] and instead prioritising cannabis users to whom they could administer formal warnings, cautions and PNfDs (often unlawfully)[58] which raised disposal numbers and maintained high 'clear-up' rates. Meanwhile, a specialist team of officers

[51] See chapters 2.2 and 4.2 of this research.
[52] See chapter 2.4 of this research.
[53] See chapter 4.2 of this research
[54] N. Cope, 'Intelligence led policing or policing led intelligence'? (2002) 44(2) British Journal of Criminology 188, 191
[55] See chapter 4.3 of this research
[56] Her Majesty's Inspectorate of Constabulary, 'Crime Recording in Kent' (2013)
[57] Ibid, 16
[58] Ibid, 19 – 20

engaged in a pro-active preventative scheme to tackle burglary found themselves reassigned to issue formal cautions to shoplifters.[59]

What emerges from this research is that there is significant evidence to suggest that the police have amassed a vast repository of criminality data but do not appear to be using it for the purpose it was primarily intended. Indeed, despite having repeated opportunities to do so in each of the cases brought against them relating to the allegation that PHOENIX data was being held 'excessively', the police were either unable, or unwilling, to demonstrate precisely how this mass of data actually assists them in preventing and/or detecting crime. Instead, they relied, and continue to rely, on anecdotal examples of how a particular piece of data assisted in a case or other, extremely weak rationale, such as a record placing an individual in a particular place at a particular time.[60]

It is very difficult, therefore, to accept at face value the police assertion as to the usefulness of this data, and it is submitted that the reality is that criminal record data plays little, if any, operational part in police investigations save for the limited uses identified in this research. The Court of Appeal in the *Five Constables* case insisted that the police be permitted to collate and retain data so long as the rationale is 'reasonable and rational'. It must now be time for the police to provide actual evidence of the 'reasonable and rational' actual, rather than theoretical use, of the data. Continuing to defer to the police as to the 'operational usefulness' of the data is not, it is submitted, acceptable in light of the legal constraints placed upon them by both the data protection legislation and the ECoHR.

Recommendation 6

An independent review ought to be conducted into the actual use of criminal records data by the police in the prevention and detection of offences. The purpose of this review should be to determine precisely how the data is being used and how effective it is in those uses. Police anecdotal reports will have some bearing on determining these but should not be decisive; an attempt should be made to establish a quantitative measure of utility to justify the retention of records under the present policy.

Even if it is accepted that data relating to recidivistic offenders *might* have some operational use for police, and further accepting that such data will nonetheless have a

[59] Ibid, 5
[60] See chapter 7.5 – 7.6 of this research.

continuing utility in the criminal justice system[61] or for disclosure purposes,[62] then the most pertinent question must be whether the data has any value where it relates to offenders who have desisted from offending. This research has highlighted that there is a criminological consensus that most offences are committed by juveniles or young adults and that most offenders desist from offending once they reach age thirty. This holds true even among those who are quite persistent offenders in their youth – the number of offences committed do not indicate a lengthy recidivistic nature unless they continue long into adulthood.[63]

The net result is that there must be literally millions of records on PHOENIX which are effectively in abeyance in that they have not been added to or amended in any way for years, and in many cases, for decades. This is likely the basis for the 40/20 rule in Scotland, where such records are simply deleted as they are deemed to offer little, or no, further operational use to police officers.[64] The deletion of these records is not perceived in Scotland to have any contrary effect on the validity of their vetting processes, which are identical to England and Wales except that the deleted records cannot be disclosed, or on their operation of the criminal justice system, where such deleted records are not considered useful for sentencing or character purposes.

It is submitted that the research shows that these old, inactive records must have an extremely limited use for policing purposes, and certainly much less use than those which show that an individual is a recidivistic offender. Except in very limited circumstances, once a record is inactive for a sufficiently lengthy period of time, the presumption must be that the individual has desisted from offending and is, therefore, of very little operational interest to the police or the criminal justice system generally. If this position, based on an extensive criminological evidence base, is not correct, then it is submitted that the onus is on the police to show otherwise and justify their 100-year retention period as not 'excessive'.

This is especially pertinent in light of the judicial trends highlighted in chapter nine of this research. The position taken in the *Five Constables* case must be now viewed against a backdrop of continued incursion into the fields of related criminality data by challenges

[61] See chapter 4.4 of this research.
[62] See chapter 8.5 of this research.
[63] See chapter 8.4.3 of this research.
[64] See chapter 8.4.2 of this research.

brought under Article 8 of the ECoHR. These have seen successful limitations placed on biometric criminality data and custody image data, so that only the PHOENIX data remains entirely under the discretion of the police.

The Home Office continues to take solace in the repeated deference to the police afforded by domestic jurisprudence,[65] but this has proven almost entirely misplaced. The ECtHR has repeatedly declared that the interpretation of Article 8 by the appellate judiciary in England and Wales to be incorrect, and that various data retention policies implemented by the police (or by the Legislature) are in violation of the protection afforded by the ECoHR.

Further illustration was provided as this research was being compiled, when the ECtHR made their determination on the appeal brought in the case of *Catt.*[66] This author had suggested that the ECtHR would take a 'less flexible view' than that taken by the Supreme Court in that case and that analysis was shown to be correct when, in January 2019,[67] the UK was found to be in violation of Article 8 in allowing the police to retain Mr. Catt's data. The judgment in that appeal was handed down rather too late for detailed consideration as part of this research, but it perhaps suffices to highlight some important principles which might be brought to bear in a future challenge to the PHOENIX collection.

The ECtHR highlighted once more that data protection principles will naturally interlink with Article 8, particularly so far as collections of criminality data by the state are concerned and the appellate courts of the UK should have that in mind, and be prepared to afford greater protection to special categories of personal data, such as criminal records data.[68] The critical question when determining whether such a data collection satisfies a 'pressing social need' is not whether the establishment or maintenance of the database is itself necessary, but rather whether the collation and retention of the data being maintained is justified.[69]

There are two fundamental, separate but interlocking considerations. Data may be legitimately collected initially, and then assessed as to its usefulness and therefore

[65] Above n.25, Annex C
[66] See chapter 9.3 of this research.
[67] *Catt v The United Kingdom*, 24 January 2019 App. No. 43514/15
[68] Ibid [112]
[69] Ibid [116]

retained for a period of time as there is a 'pressing need' to do so[70] but a violation of Article 8 may occur where the data is retained beyond the point where the 'pressing need' to hold it has passed.[71] It was on this basis that the Court held a violation in Mr. Catt's case, because although the MOPI Guidelines offered a process for considering the future deletion of the data:

> Where a state chooses to put in place such a system, the necessity of the effective procedural safeguards becomes decisive. Those safeguards must enable the deletion of any such data, once its continued retention becomes disproportionate.[72]

It is not difficult to envisage the applicability of that principle to a successful challenge against the retention of old, minor and inactive PHOENIX nominal listings.

This is the latest in a line of ECoHR jurisprudence which strengthens, it is submitted, the likelihood of a successful future challenge to the current regime for retention of criminal records data. The key issues which will determine that challenge is whether the 'until age 100 years' retention period is proportionate to the legitimate aims of crime prevention and detection and the function of the criminal justice system[73] and whether there is a 'pressing need' to retain all data for that period. In light of the findings in chapter 8.4 of this research, it is submitted that the ECtHR are likely to find that retaining all data is disproportionate and not required to meet a 'pressing need', particularly so far as arrest data, cautions, reprimands, warnings and minor conviction data is concerned, and even more so where there is a lengthy 'clear' period since the last disposal which indicates desistence or where the record largely consists of juvenile offences. The Home Office and the NPCC might consider it advisable to revisit their policy now, rather than expending resource fighting litigation it is unlikely to successfully defend. As both have failed repeatedly in the past to make concessions of their own accord, and to legitimise the process, it is submitted that issue be considered by Parliament before any new regime be implemented.

---

[70] Ibid [117]
[71] Ibid [119]
[72] Ibid
[73] Any attempt to defend the action on the basis of the need to retain data for vetting purposes is almost certain to fail; the Government have recognised that certain information has no relevance for vetting purposes (see chapter 8.5 of this research) and even the ACRO Criminal Records Office have re-instated a 'step-down' procedure for vetting outwith the statutory DBS system – see National Police Chief's Council, 'ACRO Criminal Records Office, Step Down Model, Filtering of offences for Certificates of Convictions' (5 January 2018)

Recommendation 7

It is recommended that an independent review be conducted into the retention of criminal records data. The purpose of that review should be to advise Parliament as to the optimum retention periods for criminal record data, concurrent with legitimate police and criminal justice system operational requirements and proportionately struck against data protection legislation and human rights considerations.

The review should be an independent one. It should consult widely with all possible stakeholders, including the NPCC, the Home Office, HM Courts and Tribunals Service, social services, academics, civil liberty groups and the Information Commissioner as a minimum base. The view of the police is important, and reference should be made to the findings of the report produced per recommendation 6 of this research, but they should not be decisive in determining what the optimum retention period is.

In light of the consistent failure of the appellate courts in England and Wales to properly apply the European jurisprudence to criminality data collections, the review should not, as occurred during the previous 'independent' review commissioned by the Government, simply defer to the decision in the Five Constables case.

A new review should, at the very least, consider the possibility that some records be deleted. Particular attention should be given towards arrest records, out-of-court disposals and summary court convictions which do not result in the imposition of a custodial sentence, along with disposals issued when the data subject is a juvenile. The review should consider whether there it would be proportionate to delete such records after a sufficient 'clear period' passes that indicates that the individual has desisted and so is highly unlikely to be relevant to future police or court operational processes. The review should further consider what such a clear period might be, based on empirical evidence where possible.

Recommendation 8

Upon receipt of the report recommended above, the Government should present primary legislation to give full statutory footing to a new retention regime concurrent to the recommendations made in the independent review. This statutory regime should be

similar in nature to that provided for the collation, storage and retention of biometric data.[74] The new legislation should also include an independent oversight to ensure compliance with the new regime. The Information Commissioner, armed with the strengthened regulatory powers provided to her/him in 2018, might be best placed to provide this oversight but other alternatives, such as the creation of a 'Police Ombudsman', should also be considered.

10.5 Looking to the LEDS and the LED: some concluding remarks

The PNC is, at the time of writing, forty-six years old and, save for the upgrade to PNC2 in 1991,[75] is effectively still running on the same hardware as when it was built in 1973.

In March 2016, to almost no fanfare whatsoever and buried among the latter pages of a Home Office publication on 'crime prevention strategy',[76] the Home Secretary revealed that it was planning to switch off both the PNC and the PND and intended to replace both, combined with the system for automatic number plate recognition, with a new, single online 'platform' called the Law Enforcement Data Service ('LEDS').[77] This, according, to the minister, meant that the police would be able to perform advanced 'data analytics' because 'we need to help the police forces and their partners handle and use data as easily as companies or members of the public…to help prevent crime'.[78] One suggested technique was to deploy officers to 'known hotspots' as part of 'predictive policing'.[79]

The programme to build the LEDS was called the 'National Law Enforcement Data Programme' ('NLEDP').[80] Civil libertarians were alarmed; *The Register* immediately proclaimed the project as an attempt by the 'police [to] create a mega crime database to rule them all'.[81] Concerns are exacerbated by the shroud of secrecy surrounding the project; there appears to have been precisely no Parliamentary scrutiny on the NLEDP and information in the public domain concerning what is being done, by whom and how is very sparse indeed.

---

[74] See chapter 9.4 of this research.
[75] See chapter 3.2 of this research.
[76] Home Office, Modern Crime Prevention Strategy' (March 2016)
[77] Ibid, 38
[78] Ibid
[79] Ibid
[80] H.C. Deb 15 December 2016, vol.618, col.61WS
[81] K. Hall, 'Police create mega crime database to rule them all. Is *your* numberplate in it? Could be' *The Register* (London, 23 March 2016)

What this author has been able to determine is that the programme is being led by the Home Office, though the police have designated their PNC, PND, ANPR and BCD lead officers to the 'reference group' tasked with overseeing the project.[82] The Government is providing significant public funding to finance it; in September 2016, the Home Office estimated that some £518,300,000 would be required over the lifetime of the LEDS[83] and indeed the cost of merely building the system has been put at £430m.[84] Applications are being developed by software company IBM (at a cost of £12m)[85] but details on precisely what these will consist of do not appear to be in the public domain. It is intended that the system will be fully operational by 2020.[86]

There is little doubt that the police need more up-to-date technology to help fight modern crime and criminals. Chief officers are clearly supportive and believe that the LEDS will enable a far better, quicker and more efficient sharing of data across the country.[87] Relying on systems from the 1970s is clearly inadequate; a Commons Committee in 2018 concluded that 'police forces' investment in and adaption of new technology is, quite frankly, a complete and utter mess'.[88] In theory, LEDS should help solve long-standing operational data sharing problems. It could also provide a very timely opportunity to take a 'clean-slate' approach to the longstanding problems of data quality, storage, retention and oversight, supported by new policies drafted after a comprehensive public and Parliamentary consultation ensuring compliance with the ECoHR and modern data protection legislation. The Home Office clearly thinks that the latter is a formality; it 'confirmed' DPA 2018 compliance for the LEDS in Parliament in November 2018.[89]

The basis of that pronouncement was the findings of the 'first in an annual series of LEDS privacy assessments' conducted by the Home Office in July 2018.[90] This Privacy Impact Assessment ('PIA') is perhaps the only document in the public domain which provides any

[82] 'Chief Constables Project, EMSCP and NLEDP Update' (14 July 2016) Agenda item: 4.3.1
[83] Home Office, 'Transparency Data: HO Government Major Project Portfolio data, September 2016' (18 July 2017)
[84] R. Anderson and R. Stoneman, 'GlobalData on Home Office funding for the law enforcement data programme' *Government Computing* (London, 23 November 2018)
[85] Home Office, 'Home Office (HO) National Law Enforcement Data Programme (NLEDP) Application Development Service. Tender Application' (28 October 2016)
[86] Above n.26
[87] Home Affairs Committee, *Policing for the Future* (HC 515 2017 – 19, 10 – I) Oral evidence at Q485
[88] Ibid, para.186
[89] HC Written Question 185654, October 30 2018
[90] Home Office, 'National Law Enforcement Data Programme: Law Enforcement Data Service – Privacy Impact Assessment Report' (July 2018)

detail on what the LEDS will be once it is operational and is the first time that any PIA has ever been conducted in respect of the PNC and it's data.[91]

The Home Office claims that it intends to 'privacy-friendly, not just privacy-compliant'.[92] To this end, the ICO were consulted and 'ongoing liaison' was intimated.[93] However, scrutiny of the document reveals immediate potential problems. The PIA confirms that all of the data from the PNC and the PND is to be migrated onto LEDS,[94] which clearly risks the importation of poor quality data and will certainly include all of the arguably excessive data highlighted in this research. It is intended to mark all LEDS data as 'OFFICIAL', rather than 'SENSITIVE'.[95] This will allow far greater access to the data, internally and externally and potentially via mobile devices, and is not, it is submitted, concurrent with the nature of data specifically described in the DPA 2018 as 'sensitive personal data'.

Interestingly, the PIA recognises that 'although the retention periods for arrest, conviction and caution data has been subject to legal challenge' but that the continued retention of it 'was confirmed by the Court of Appeal in 2009', that

> Nevertheless, it is recognised that the retention of information concerning those arrested but not charged or who are charged but subsequently not convicted of any offence and who have no previous convictions could be seen as disproportionate in the context of data protection, as could the retention of a number of old records relating to individuals with a small number of minor historical offences with no recurrence which have been retained.[96]

Following this, it is then claimed that 'the retention of arrest only records is currently under review with consideration being given to the removal of a number of such records from the system'.[97] Who is conducting this 'review', what the terms of reference are for it or when it is expected to conclude is not specified but the publication of the findings are certainly to be eagerly anticipated. The PIA then further notes that the moving of both PNC and PND data to LEDS 'may be an opportunity to devise a single retention regime, based

[91] Ibid, 7
[92] Ibid, 9
[93] Ibid
[94] Ibid, 5
[95] Ibid, 11 – 12
[96] Ibid, 20
[97] Ibid, 21

on the MOPI code of practice, for the application of all police data on the platform'.[98] Were this to be done it could result in one of two possible outcomes; either large chunks of PNC data will have to be reviewed and potentially deleted because the current retention policy for this is scrapped, or, alternatively, large tranches of PND data which would otherwise have been deleted will be retained because it is decided to make the current PNC retention guidance applicable to all LEDS data.

While potentially useful on paper, there is, however, some considerable doubt as to whether the police will actually use the LEDS for anything other than an opportunity to collate and retain yet more data, this time on one, rather than disparate, databases. There remains no proposal to introduce a statutory framework for the collation, storage and retention of data on the LED comparable to that for biometric data (and which this author believes will inevitably be need to be introduced regarding custody images if the current process is not revisited) and there are no proposals to introduce effective, independent oversight of the use of the LEDS. The charge must be laid, therefore, that in reality, the LEDS will simply be 'business as usual', so far as criminal records data is concerned.

More concerningly, such a charge might transpire to be the best-case scenario. It has now become clear that the police intend to press ahead with proposals to include their collection of custody images on the LEDS as a searchable feature, albeit now linked to all of the data currently held on the PND and PNC.[99] This is despite continued reservations as to the lawfulness of that collection and the refusal of the Government to yield to calls to revisit their 2017 Custody Image Review; in fact, they have even refused to furnish the Commons Science and Technology Committee with a copy of their legal advice on their new custody image deletion process, retreating instead behind legal professional privilege.[100] One Parliamentarian told a House of Lords debate that they feared that 'without regulation or oversight there is the potential for Nineteen-Eighty Four to become a reality, albeit 34 years later than originally envisaged'.[101]

---

[98] Ibid, 25

[99] H.L Deb 1 March 2018, vol.789, cl.793

[100] 'Government's Response to the House of Commons Science and Technology Committee: Biometrics strategy and forensics services'' (HC 800, 2017 – 19, 5 – I)

[101] Above n.41, col.805. Indeed, in the days before this research was due for submission, a legal challenge has been brought against the police relating to their use of facial recognition software. It would be something of a surprise if this was not ultimately successful, albeit that a hearing in the ECtHR might be required to resolve the matter: see C. Coleman, 'Police facial recognition surveillance court case starts' *The BBC* (London, 21 May 2019)

Rather more alarmingly, on 1 October 2018 *Liberty* removed itself from the 'Open Space Consultation' Group established to consider the privacy impact of the LEDS. In an open letter to the Home Office, it offered a damning assessment of the privacy ramifications for the proposals the Home Office were outlining; the system did not have an agreed retention policy for the data being moved to it, that data which is being held which the Home Office know to be unlawful was being migrated to LEDS nonetheless and the Home Office were proposing to provide access to non-police organisations where a 'business case' is made out. This led *Liberty* to reach a conclusion that they had to withdraw, warning that:

> a new policing super-computer is in the works – and it puts our rights at serious risk. The Home Office has failed to respond sufficiently to Liberty's concerns. We can't be part of a process that gives a free pass to the creeping expansion of digital policing that shows contempt for our privacy rights.[102]

In spite of these concerns, and further concerns from a Commons Committee that the project is 'welcome, though woefully unambitious',[103] the Home Office is pressing ahead with the development of the LEDS. It is submitted that there is perhaps a need to pause and to consult, before it reaches a point of no-return. The lack of information being provided to the public and to Parliament remains a significant concern. It is submitted that the sooner the Home Office and the police begin to inform the public about what they are doing, and what safeguards they are putting in place to protect the rights of data subjects, the less likely they are to face foreseeable legal challenges relating to the LEDS in the immediate future.

In the *Five Constables* case, Waller LJ dismissed data protection generally as 'a sidewind'.[104] Whether he was correct in 2009 to describe data protection as such is a debate for a different piece of research, what is abundantly clear is that such a description is not apt in 2019. In fact, with the possible exception of the UK's impeding departure from the European Union, data protection has dominated the legal and economic discourse over the life of this research to a hitherto unprecedented degree.[105]

---

[102] H. Couchman, 'Why we're no longer taking part in a consultation on the police's new super-database' *Liberty* (1 October 2018)
[103] Above n.33, 63
[104] [2009] EWCA Civ 1079 [44]
[105] At the time of writing, 'data protection remains in the news'; S. Stokes, 'Data protection, information security and cloud computing' (2019) 163 (Feb) Compliance Officer Bulletin 1

The responsibility for what one author describes as 'much hullabaloo'[106] lies almost entirely with the implementation of the General Data Protection Regulations ('GDPR')[107] which repealed the 1995 EU Directive on Data Protection on 25 May 2018.[108] The GDPR is the European Union's attempt to completely harmonise data protection provisions across all member states, offering a 'consistent and high level of protection' to all EU citizens[109] and was enacted to address the enormous growth in the collation, flow and utilisation of personal data by electronic means (particularly as regards the internet) which was simply not in contemplation when the 1995 Directive was passed.[110] The internet has turned data into a valuable commodity – one commentator has described it as 'the oil of the internet' – and 'big data' is now a multi-billion pound industry.[111] The GDPR was enacted to redress some of the balance back towards the data subject[112] and the implementation of a Regulation rather than a Directive, meant that harmonisation was to be achieved by provisions which had direct effect in all member states.[113]

The GDPR, however, do not apply to 'the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties'.[114] Instead, criminal record data is to governed by the Law Enforcement Directive ('LED')[115], which operates alongside, but not part of, the GDPR. This recognises that 'the scale of the collection and sharing of personal data has increased significantly. Technology allows personal data to be processed on an unprecedented scale…' so far as police operational processes are concerned[116] and the LED intends 'to harmonise protection for all EU citizens whilst facilitating judicial co-operation and police data-sharing throughout the EU'.[117]

[106] T. Morrison, 'Mind the GDPR (part 5)' (14 September 2018) 168 New Law Journal 7808, 14
[107] Regulation (EU) 2016/679, 27 April 2016
[108] Ibid, Chapter XI, Article 94, s.1
[109] Ibid, para.10
[110] Ibid, para.5.
[111] V. Bishnoi, 'Data Protection Law: an inhibition in enforcement and promotion of competition law' (2019) 40(1) European Competition Law Review 34 – 40, 40
[112] Ibid
[113] Regulations have 'Direct Effect' – that is to say that they are immediately incorporated into law in all EU member states on the date of applicability. By contrast, each member state is afforded an opportunity to bring into domestic law in a manner of their choosing (so long as it is effective in doing so) any Directive which is passed by the EU.
[114] Above n.107, para.19
[115] Directive (EU) 2016/680, 27 April 2016
[116] Ibid, para.3
[117] Ibid, para.7

The LED applies to the processing of criminal record data by a 'competent authority', which expressly includes the police.[118] This clearly indicates that PHOENIX now falls under the ambit of LED, rather than the GDPR. It is perhaps worth noting that there is nothing in the LED which provides that states can (or cannot) compile and retain a record of all criminal convictions against individuals. It does, however, state that 'a clear distinction, where applicable and as far as possible, be made between personal data of different categories of data subjects such as; suspects and persons convicted of a criminal offence'.[119] A supervisory body is required to oversee compliance[120] and one instituted to ensure compliance with the GDPR may also fulfil this purpose. The Information Commissioner remains, therefore, the official supervisory authority for criminal record data.

The LED required that member states publish laws which brought the LED into national law by 6 May 2018.[121] The UK Parliament waited a little longer, and implemented the Data Protection Act 2018[122] ('the DPA 2018') on 25 May 2018; the same date that the GDPR came into force. The DPA 2018 repealed the DPA 1998 almost entirely[123] and runs parallel to GDPR, intended to supplement one another and both being applicable simultaneously. Unlike GDPR, however, the DPA 2018 does apply to criminal records, as Part 3 of the Act intends to bring into domestic law the provisions of the LED.[124]

Part 3 of the DPA 2018, entitled 'Law Enforcement Processing', contains the legal provisions which are now applicable to the collection of criminal records currently on PHOENIX (and soon to be transferred to the LEDS).[125] This provides for six applicable Data Protection Principles.[126] These look rather familiar; processing has to be, *inter alia*; 'lawful and fair',[127] for a specified, explicit and legitimate purpose,[128] 'accurate and kept

[118] Ibid, para.11
[119] Ibid, para.31
[120] Ibid, para.76
[121] Ibid, Article 63, para.1
[122] 2018, ch.12
[123] Ibid, Schedule 19, Part.1, s.44
[124] Ibid, s.1(3)
[125] Per s.29(1) DPA 2018, the provisions apply 'to processing by a competent authority wholly or partly by automated means', where the police are the 'competent authority' and the PNC/LEDS is the 'automated means'.
[126] Ibid, s.34
[127] Ibid, s.34(1)(a)
[128] Ibid, s.34(1)(b)

up-to-date',[129] securely stored[130] and, most pertinently to this research, 'adequate, relevant and not excessive'[131] and 'not kept for longer than is necessary'.[132]

Interestingly, in among the numerous subsequent provisions which offer guidance and further provision regarding each of these data principles, s.37 of the DPA 2018 does nothing more than simply repeat the principle; Parliament has offered no further guidance, clarification or definition whatsoever. As regards the requirement that data not be kept for longer than is necessary, the DPA 2018[133] provides that 'appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any law enforcement data'. It is submitted that the police are therefore in *prima facie* breach of the fifth Data Principle, as the current retention regime for the PHOENIX data offers no review periods whatsoever. One might expect the Information Commissioner to be considering enforcement action, considering the significantly expanded powers afforded to him by the DPA 2018.[134]

In truth, neither the LEDS nor the DPA 2018 materially affect the present unsatisfactory state of affairs regarding the criminal record collection. The LEDS affords the police and the Home Office an opportunity to implement a new regime for data collation, storage and retention. Early indications are that they do not intend to take it. The DPA 2018 is likely to provide the new backdrop to challenges against the police record retention regime, but the fundamental tenets of these are likely to remain the same.

The recommendations made in this research would, if implemented, alleviate some of the problems and potentially head off fresh legal challenges. In any event, the status quo simply cannot be maintained. The next developments in criminal record data law are awaited, by this author and around twelve million other citizens in England and Wales, with considerable interest.

[129] Ibid, s.34(1)(d)
[130] Ibid, s.34(1)(f)
[131] Ibid, s.34(1)(c)
[132] Ibid, s.34(1)(e)
[133] Ibid, s.39(2)
[134] Ibid, Part 6

Bibliography

Academic Texts

Agar J, *The Government Machine: A Revolutionary History of the Computer* (The MIT Press 2003)

Aislabie W I, *The Ticket-of-Leave System in Australia and England* (Vol.1, Effingham Wilson, London 1857)

Allott P, *The Health of Nations: Society and Law Beyond the State* (Cambridge University Press 2002)

Ashbaugh D, *Quantitative–Qualitative Friction Ridge Analysis: an introduction to basic and advanced Ridgeology* (CRC Press 1999)

Bailey D, *Policing for the Future* (Oxford University Press 1994)

Barr R, *The Scotland Yard Story* (Hodder and Stoughton 1962)

Beatie J M, *The First English Detectives: The Bow Street Runners and the Policing of London, 1750 – 1840* (Oxford University Press 2012)

Brain T, *A history of policing in England and Wales from 1974: a turbulent journey* (Oxford University Press, 2010)

Brogden M, *The Police: Autonomy and Consent* (Academic Press Inc. 1984)

Bullock K and Tilley N, *Crime Reduction and Problem-Oriented Policing* (Willian Publishing 2003)

Cahillane L and Schweppe J, *Legal Research Methods: Principles and Practicalities* (Clarus Press 2016)

Campbell D and Connor S, *On the Record – Surveillance, Computers & Privacy* (Michael Joseph 1986)

Cane P and Kritzer H M, *The Oxford Handbook of Empirical Legal Research* (Oxford University Press 2012)

Cole S, *Suspect identities: a history of fingerprinting and criminal identification* (Harvard University Press 2001)

Collins P, Ricks T A & van Meter W, *Principles of Security and Crime Prevention* (Routledge London 2015)

Colquhorn P, *Treatise on the Police of the* Metropolis (7th edn, Patterson Smith Publishing 1806)

Cotterrell R, *Law's Community: Legal Theory in Sociological Perspective* (Clarendon Press 1995)

Cownie F, *Legal Academics: Culture and Identities* (Hart Publishing 2004)

Craib R, *The Cry of the Renegade: Politics and Poetry in Interwar Chile* (Oxford University Press 2016)

de Cruz P, *Comparative Law in a Changing World* (2nd ed, Cavendish 1999)

Dilnot G, *Scotland Yard: the methods and organisation of the Metropolitan Police* (Marschall London 1915)

Doss D *et al*, *Economic and Financial Analysis for Criminal Justice Organisations* (CRC Press 2014)

Du Cane E F, *The Punishment and Prevention of Crime* (Read Books 2013)

Dunston G J, *Whores and Highwaymen: Crime and Justice in the Eighteenth-Century Metropolis* (Waterside Press 2012)

Emsley C, *The English Police: A Political and Social History* (Routledge 2014)

Farrell G and Pease K, *Repeat Victimisation: Crime Prevention Study Series 12* (Monsey, Criminal Justice Press 2001)

Fosdick R B, *European Police Systems* (The Century Co 1915)

Galton F, *Fingerprints* (MacMillan and Co: London 1892)

Garner B A, *Black's Law Dictionary* (9th edn, Thompson Reuters 2009)

Gill P, *Rounding up the Usual Suspects? Developments in Contemporary Law Enforcement Intelligence* (Aldershot: Ashgate 2000)

Gladfelder H, *Criminality and Narrative in Eighteenth-Century England: Beyond the Law* (John Hopkins University Press 2001)

Glover Alexander G, *The Administration of Justice in Criminal Matters (in England and Wales)* (Cambridge University Press 1915)

Godfrey B S, Cox D and Farrall S, *Serious Offenders: a historical study of habitual offenders* (Oxford University Press 2010)

Goldson B and Muncie J, *Youth Crime and Justice* (Sage 2006)

Gorer G. *Exploring English Character* (Cresset, London 1955)

Halsbury's Laws of England, *Criminal Procedure* (2015)

Harrison B, *Finding a Role? The United Kingdom 1970 – 90* (Oxford University Press 2011)

Hawkins K (ed) *The Human Face of Law: Essays in Honour of Donald Harris* (Oxford University Press 1997)

Higgs E, *The information state in England* (Palgrave MacMillan 2004)

– – *Identifying the English: A History of Personal Identification 1500 to the present* (Continuum Publishing 2011)

Holder E, T*he Fingerprint Sourcebook* (National Institute of Justice 2011)

Houck M M, Forensic Fingerprints (Elsevier 2016)

Hueske E E, *Firearms and Fingerprints* (Infobase Publishing 2009)

Innes J, *Inferior Politics: Social Problems and Social Policies in Eighteenth Century Britain* (Oxford University Press 2009)

Jackson J *et al*, *Just Authority? Trust in the Police in England and Wales* (Routledge 2013)

Johnson H, *Crime in England 1815 – 1880: Experiencing the Criminal Justice System* (Routledge 2015)

Joyce P, *Criminal Justice: An Introduction* (Routledge, Oxford 2017)

Jupp V, *Methods of Criminological Research* (Routledge 1999)

Kamilah Muda A *et al*, *Computational Intelligence in Digital Forensics: Forensic Investigation and Applications* (Springer 2014)

Kroener I, *CCTV: a technology under the radar?* (Routledge 2014)

Lacey N, *A reader in Criminal Justice* (Oxford University Press 1994)

Lammasniemi L, *Law Dissertations. A Step-by-Step Guide* (Routledge 2018)

Liebling A, Maruna S and McAra L, *The Oxford Handbook of Criminology* (Oxford University Press 2017)

Lister S and Rowe M, *Accountability of Policing* (Routledge 2016)

Mair G and Burke L, *Redemption, Rehabilitation and Risk Management: A History of Probation* (Routledge 2012)

Malz M D, *Recidivism* (Academic Press Inc, Florida 2001)

Marshall D and Thomas T, *Privacy and Criminal Justice*, (Palgrave MacMillan 2017)

Martienssen A, *Crime and the Police* (Penguin 1953)

Matthews C, *The Police Code and General Manual of the Criminal Law* (15th edn, Butterworths and Co 1912)

McCartney C, *Forensic Identification and Criminal Justice* (Routledge 2012)

McConville M *et al*, *Standing Accused: The Organisation and Practices of Criminal Defence Lawyers in Britain* (Clarendon Press, Oxford 1994)

– – and Chui W H, *Research Methods for Law* (2nd edn, Edinburgh University Press 2017)

McLynn F, *Crime and Punishment in Eighteenth Century England* (Routledge 1989)

Melville Lee W L, *A history of police in England* (Methuen & Co 1901)

Moritz E, *Winston Spencer Churchill and Social Reform* (University of Winconsin 1953)

Morizot J and Kazemian L, *The Development of Criminal and Anti-Social Behaviour, Theory, Research and Practical Applications* (Springer Publishing 2015)

Morland N, *Science against Crime* (Exeter Books 1984)

Moss A and Skinner K, *The Victorian Detective* (Shire Publications 2013)

Moylan J F, *Scotland Yard and the Metropolitan Police* (G.P Putnam & Son 1929)

Newburn T, *Handbook of Policing* (Willan Publishing 2008)

– – Williamson T and Wright A, *Handbook of Criminal Investigation* (Willan Publishing 2008)

O'Toole S, *The History of Australian Corrections* (UNSW Press 2006)

Palmiotto P & Prahba Unnithan N, *Policing and Society, A Global Approach* (Delmar Cengage Publishing 2011)

Pepper I, *Crime Scene Investigation: Methods and Procedures* (Oxford University Press 2010)

Petrow S, *Policing Morals: The Metropolitan Police and the Home Office 1870 – 1914* (Clarendon Press 1995)

Pratt J, *Governing the Dangerous: Dangerousness, Law and Social Change* (The Federation Press 1997)

Radzinowicz L and Hood R, *The Emergence of Penal Policy in Victorian and Edwardian England* (Clarendon 1990)

Rahn B J, *The Real World of Sherlock* (Amberley Publishing 2014)

Ralston A G, *The Real Taggarts: Glasgow's Post-War Crimebusters* (Black and White Publishing 2017)

Ratcliffe J, *Intelligence–Led Policing* (Routledge 2011)

Redmayne M, *Character Evidence in the Criminal Trial* (Oxford University Press 2015)

Rowe M, *Introduction to Policing* (Sage Publishing 2014)

Rule J, *Private Lives and Public Surveillance* (Allen Lane 1973)

Salter M and Mason J, *Writing Law Dissertations* (Pearson Longman 2007)

Samuel G, *An introduction to Comparative Law Theory and Method* (Hart Publishing 2014)

Schlesinger L B, *Serial Offenders: Current Thought, Recent Findings* (CRC Press 2000)

Scott H, *Scotland Yard* (Andre Deutsch, Lindon 1954)

Sharpley D, *Criminal Litigation, Practice and Procedure 2017/18* (College of Law Publishing 2017)

Shoemaker R, *The London Mob: Violence and Disorder in Eighteenth-Century England* (Cambridge University Press 2004)

Shpayer-Makov H, *The ascent of the detective: police sleuths in Victorian and Edwardian England* (Oxford University Press 2011)

Sprack J*, Emmins Guide to Criminal Procedure* (9th edn, OUP 2002)

Stead P J, *The Police of Britain* (MacMillan 1985)

Taylor D, *The New Police in Nineteenth Century England: Crime, Conflict and Control* (Manchester University Press 1997)

Thomas P, *Socio-Legal Studies* (Ashgate-Dartmouth 1997)

Thomas T, *Criminal Records, A Database for the Criminal Justice System and Beyond* (Palgrave Macmillan 2007)

– – *The Registration & Monitoring of Sex Offenders: A Comparative Study* (Routledge 2011)

– – *Sex Crime, Sex Offending and Society* (Routledge 2015)

– – *Policing Sexual Offences and Sex Offenders* (Palgrave 2016)

Thompson B, *The Story of Scotland Yard* (Grayson & Grayson 1925)

– – *The Story of Scotland Yard* (The Literary Guild 1936)

Thompson T and Black S, *Forensic Human Identification: An Introduction* (CRC Press 2007)

Tong S *et al*, *Understanding Criminal Investigation* (Wiley-Blackwell 2009)

Turnbull S, *The TV Crime Drama* (Edinburgh University Press 2014)

Virilio P, *The Vision Machine* (Indiana University Press 1994)

Watkins D and Burton M, *Research Methods in Law* (Routledge 2018)

Watson J A F and Austin P M, *Modern Juvenile Court* (Shaw & Sons Ltd 1975)

Weller T, I*nformation History in the Modern World: Histories of the Information Age* (Palgrave MacMillan 2011)

Wiener M J, *Reconstructing the Criminal: Culture, Law and Policy in England, 1830 – 1914* (Cambridge University Press 1990)

Williams C A, *Police Control Systems in Britain 1775 – 1975: from Parish Constable to National Computer* (Manchester University Press 2014)

Williams R and Johnson P, *Genetic Policing: the uses of DNA in police investigations* (Willian Publishing 2008)

Wilson D, *Surveillance, Crime and Social Control* (Routledge 2006)

Woodhall E T, *Secrets of Scotland Yard* (John Lane: The Bodley Head 1936)

Yount L, *Forensic Sciences: From Fibers to Fingerprints* (Chelsea House Publishers 2007)

Zweigert K and Kötz H, *An introduction to Comparative Law* (Oxford University Press 1998)

Journal Articles

– – (Jul. 1986) 47(2) The Magistrate 107

– – ‘Editorial’ (1994) 50(1) The Magistrate 20

– – ‘Regional Criminal Records’ (1961) 34 Police Journal 310

Alach Z, ‘The emperor is still naked: how intelligence-led policing has repackaged common-sense as transcendental truth’ (2011) 84(1) Police Journal 75

Arthur R, ‘The Criminal Justice and Courts Act 2015 – Secure Colleges and the Legitimation of State Sponsored Violence’ (2016) 79(1) Modern Law Review 102

Ashworth A, ‘Criminal Justice Act 2003: The Sentencing Provisions’ (2005) 68(5) Modern Law Review 822

Baldwin C, ‘Necessary Intrusion or Criminalising the Innocent? An Exploration of Modern Criminal Vetting’ (2012) 76(2) Journal of Criminal Law 140

– – ‘The Vetting Epidemic in England and Wales’ (2017) 81(6) Journal of Criminal Law 478

– – ‘The Demise of the Criminal Records Bureau’ (2019) 83(3) Journal of Criminal Law 229

Bapat A, ‘The new rules on using children’s data’ (2012) 12 (5) Privacy and Data Protection Journal 12

Bateman T, ‘Youth Justice News’ (2007) 7 Youth Justice 66

Booth N, ‘Prisoners’ families and children’ (2017) 181(15) Criminal Law and Justice Weekly 246

Branston G, ‘A reprehensible use of cautions as bad character evidence?’ (2015) 8 Criminal Law Review 594

Campbell C M and Wiles P, ‘The Study of Law and Society in Britain’ (1976) 10(4) Law and Society Review 547

Campbell L, ‘Criminal Record and Human Rights’ (2017) 9 Criminal Law Review 696

Coghlan N, ‘Gaughran [2015] UKSC 29 on biometric data retention: Strasbourg unheard, Strasbourg unheeded’ (2016) 1 European Human Rights Law Review 61

Colvin M, ‘The Criminal Record and Information System in England and Wales’ (1992) 6 International Yearbook of Law Computers and Technology 139

Cope N, ‘Intelligence-led policing of Policing-led intelligence?’ (2004) 44(2) British Journal of Criminology 188

Cowan V, ‘Probation on trial’ (2018) 182 Criminal Law and Justice Weekly 176

Darbyshire P, ‘The Law Commission Consultation Paper on previous misconduct; Part 3: Previous Misconduct and magistrates courts – some tales from the real world’ (Feb. 1997) Criminal Law Review 105

Dawson P and Stanko E, ‘The best-kept secrets of evidence-based policing’ (2016) 16(2) Legal Information Management 64

Devlin J D, ‘Procedure, Administration and Organisation: IV Police Communications’ (1966) 39 Police Journal 514

– – ‘Procedure, Administration and Organisation: VI Police Communications’ (1966) 39 Police Journal 620

Donaghue J C, ‘Reforming the role of Magistrates: implications for summary justice in England and Wales’ (2014) 77(6) Modern Law Review 928

Done F, ‘Youth Cautions: keeping children out of court’ (2012) 176(47) Criminal Law and Justice Weekly 678

Easton R, ‘The Right to be Forgotten’ (2014) 178(27) Criminal Law and Justice Weekly 408

Edwards A, ‘In Practice: Criminal Law – Conditional Cautions’ (2008) 5 Law Society Gazette 19

Edwards I, ‘Sentencing Councils and Victims’ (2012) 75(3) Modern Law Review 324

Elkins M, ‘Adult Defendant anonymity in Criminal Proceedings’ (2016) 180 Criminal Law and Justice Weekly 387

Epstein L and King G, ‘Empirical Research and the Goals of Legal Scholarship: The Rules of Inference’ (2002) 69 University of Chicago Law Review 1

Epstein R, ‘Summary Justice: fast – but is it fair?’ (2008) 172(48) Justice of the Peace and Local Government Law 791

– – ‘The Sentencing Council: what is it for’? (2017) 181 Justice of the Peace 167

Evans R and Wilkinson C, ‘Police cautioning of juveniles: the impact of the Home Office Circular 14/1985’ (Mar. 1990) Criminal Law Review 165

Farmer M, McAlinden A M and Maruna S, 'Understanding desistance from sexual offending: A thematic review of research findings' (2015) 62(4) Probation Journal 320

Farrington D, 'Official bias in Intergenerational Transmission of Criminal Behaviour' (2013) 53(3) British Journal of Criminology 438

Field S, 'Early intervention and the 'new' youth justice: a study of intensive decision making' (2008) 3 Criminal Law Review 177

Flaherty P, 'Sentencing the recidivist: reconciling harsher treatment for repeat offenders with modern retributivist theory' (2008) 8(4) Contemporary Issues in Law 319

Fosdick R, 'The Passing of the Bertillon System of Identification' (1915) 6 Journal of the Institute of Criminal Law and Criminology 363

Francis B and Soothill K, 'When do ex-offenders become like non-offenders?' (2009) 48(4) The Howard Journal of Crime and Justice 373

Gelsthorpe L and Morris A, 'Much ado about nothing - a critical comment on key provisions about children in the Crime and Disorder Act 1998' (1999) 11 Child and Family Law Quarterly 209

Gosling M, 'We know where you are' (2007) 171 Justice of the Peace 850

Gourdley J, 'Comparative Legal Research: its function in the development of harmonized law' (1995) 43 American Journal of Comparative Law 555

Grace J, 'Old convictions never die, they just fade away: the permanency of convictions and cautions for criminal offences in the UK' (2014) 78(2) Journal of Criminal Law 121

Hayes B, 'A Failure to Regulate: Data Protection and Ethnic Profiling in the Police Sector in Europe' (2005) Open Society 32

Heaton R, 'Police resources, demand and the Flanagan Report' (2009) 82(2) Police Journal 95

Hoey A, 'Techno-cops: Information Technology and Law Enforcement' (1998) 6(1) International Journal of Information Technology 69

Huseyin R, 'The Commissioner's Annual Report' (2001) 1(8) Privacy and Data Protection 1

Hynes P and Elkins M, 'Suggestions for reform to the police cautioning procedure' (2013) 12 Criminal Law Review 966

Jackson A and Davies G, ‘Making the case for ECRIS: Post-‘Brexit’ sharing of criminal records information between the European Union and United Kingdom’ (2017) 21(4) The International Journal of Evidence and Proof 330

James A, ‘The advance of intelligence-led policing’: the emperor’s new clothes?’ (2003) 76(1) Police Journal 45

Jeanes J, ‘Police Note’ (Nov. 1965) Bracton Law Journal 15

Johnson H, ‘Data Retention – scope of police powers’ (2015) 2 Communications Law 56

Jones K, ‘Disclosure of youth criminal records’ (2018) 8 Archbold Review 6

Hanson R K, ‘Long-term recidivism studies show that desistance is the norm’ (2018) 45 (9) Criminal Justice and Behaviour 1340

Kyle S, ‘Risk assessment in pre-sentence reports’ (2005) 169 Justice of the Peace 374

Naylor B, Paterson M and Pittard M, ‘In the shadow of a Criminal Record: Proposing a Just model of criminal record employment checks’ (2008) 32(1) Melbourne University Law Review 171

Naylor B, ‘Criminal Records and Rehabilitation in Australia’ (2011) 3(1) European Journal of Probation 79

Laub J H and Sampson R J, ‘Understanding Desistance from Crime’ (2001) 28 Crime and Justice 1

Lindsay R, Jackson T and Cooke L, ‘Mobile access to information systems in Law Enforcement: An Evaluation of its implications for Data Quality’ (2010) 13(2) The Electronic Journal of Information Systems Evaluation 143

Lippke R, ‘Criminal record, character evidence and the criminal trial’ (2008) 14(3) Legal Theory 167

McCrudden C, ‘Legal Research and the Social Sciences’ (2006) 122 Law Quarterly Review 632

McGee T R and Farrington D P, ‘Are there any true adult-onset offenders?’ (2010) 50(3) British Journal of Criminology 530

McKintyre T J and O’Donnell I, ‘Criminals, Data Protection and the right to a second chance’ (2017) 58 Irish Jurist 27

McMullan J, ‘Policing reform and moral discourse: the genesis of a modern institution’ (1998) 21 (1) Policing: An International Journal of Police Strategies and Management 137

Miller J, ‘News – Long wait to check staff criminal records’ (2005) 155 New Law Journal 1230

Morgan R, ‘What’s the Problem?’ (2007) 157 New Law Journal 305

Morris A, ‘Critiquing the Critics’ (2002) 42(3) British Journal of Criminology 596

Morrison, ‘Mind the GDPR (part 5)’ (2018) 168 New Law Journal 7808

Munday R, ‘Round up the usual suspects! Or what we have to fear from Part 11 of the Criminal Justice Act 2003’ (2005) 169 Justice of the Peace 328

Mustafa N *et al*, ‘An exploration of the historical background of criminal record checking in the United Kingdom: from the eighteenth to the twenty-first century’ (2013) 19 European Journal of Criminal Policy and Research 15

Newburn T and Reiner R, ‘From PC Dixon to Dixon PLC: policing and police powers since 1974’ (Aug. 2004) Criminal Law Review 601

Oswald M, ‘Joining the dots – intelligence and proportionality’ (2013) 13(5) Privacy and Data Protection Journal 6

Palfrey W, ‘Police Communications’ (1961) 34 Police Journal 79

Pendleton M, ‘Non-empirical discovery in legal scholarship – Choosing, Researching and Writing a Traditional Scholarly Article’ (2007) Research Methods for Law 159

Pijoan E L, ‘Criminal record disclosure and the right to privacy’ (2014) 10 Criminal Law Review 723

Pitt Payne T, ‘Employment: the shadow of the past’ (2009) 159 New Law Journal 1530

Pope N, ‘Intelligence led policing or policing led intelligence?’ (2004) 44(2) British Journal of Criminology 188

Postner R, ‘The Decline of Law as an Autonomous Discipline: 1962 – 1987’ (1987) 100 Harvard Law Review 761

Pounder C N M, ‘Data Protection and the Police’ (1983) 10 Journal of Law and Society 109

Puech K and Evans R, ‘Reprimands and warnings: populist punitiveness or restorative justice?’ (Oct. 2001) Criminal Law Review 794

Purshouse J, ‘Non-conviction disclosure as part of an enhanced criminal record certificate: assessing the legal framework from a fundamental human rights perspective’ (Oct. 2018) Public Law 668

Redmayne M, ‘The relevance of bad character’ [2002] 61 The Cambridge Law Journal 684

Reed K, ‘Retaining DNA’ (2015) 179 Criminal Law and Justice Weekly 514

Roberts J, ‘Sentencing guidelines and judicial discretion’ (2011) 51(6) British Journal of Criminology 997

– – ‘Punishing Persistence’ (2008) 48(4) British Journal of Criminology 468

Robson G, ‘The art of sentencing’ (2009) 173 Justice of the Peace 453

Rose D, ‘Overview of the week’ (2017) 181 Justice of the Peace 192

Rozenberg J, ‘Columnist: matters of discretion’ (2008) 10 Law Society Gazette 18

Santos *et al,* ‘Forensic DNA databases in European countries: is size linked to performance?’ (2013) 9 Life Sciences, Society and Policy 12

Selbin J *et al*, ‘Unmarked: Criminal Record Clearing and Employment Outcomes’ (2018) 108(1) Journal of Criminal Law and Criminology 5

Sherman L and Weisburd D, ‘General Deterrent Effects of Police Patrol in Crime Hotspots: a randomised control trial’ (1995) 12 Justice Quarterly 626

Shoemaker R & Ward R, ‘Understanding the criminal: record-keeping, statistics and the early history of Criminology in England’ (2017) 57 The British Journal of Criminology 6 1442

Smith D J, ‘Mr. Lustgarden and the case of the honest copper’ (1998) 8(3) Oxford Journal of Legal Studies 434

Sodhi G S and Kaur J, ‘World’s First Conviction on Fingerprint Identification’ (2003) 15(2) National Crime Records Bureau Gazette 1

Soothill K *et al*, ‘What is the future repeat danger from sexual offenders against children? Implications for policing’ (2005) 37 Police Journal 78

Spencer J R, ‘Evidence of bad character – where are we today?’ (2014) Archbold Review 6

Stark F, ‘Wiping the slate clean: reforming Scots Law’s approach to evidence of the accused’s bad character’ (2013) 76(2) Modern Law Review 346

Steer D, ‘The Elusive Conviction’ (1973) 13 British Journal of Criminology 373

Stokes S, ‘Data protection, information security and cloud computing’ (2019) 163 (Feb) Compliance Officer Bulletin 1

Suff R, ‘Checking out the activities of the Criminal Records Bureau’ (2005) 828 IRS Employment Review 42

Telford M, ‘Youth justice: new shoots on a bleak landscape – Director of Public Prosecutions v P’ (2007) 19(4) Child and Family Law Quarterly 505

Thomas T, ‘The Exchange of information between the police and social services departments’ (1986) 8(4) Journal of Social Welfare and Family Law 215

– – ‘Criminal record of police record?’ (2000) 150 New Law Journal 1629

– – ‘National collection of criminal records – a question of data quality’ (Nov. 2001) Criminal Law Review 886

– – ‘Employment Screening and the Criminal Records Bureau' (2002) 31(1) Industrial Law Journal 55

– – ‘Much ado about MAPPA’ (2011) 175 Justice of the Peace 755

Treacy B and Terelgas A, ‘Under the spotlight: police retention of conviction data’ (2010) 10 (3) Privacy and Data Protection Journal 12

Turner A, ‘Respect and Responsibility’ (2003) 167 Justice of the Peace 221

– – ‘Protecting Children Effectively’ (2009) 173 Justice of the Peace 290

Uglow S, ‘Criminal records under the Police Act 1997’ (Apr. 1998) Criminal Law Review 235

Vere van Koppen M, ‘Criminal Career Dimensions of juvenile and adult-onset offenders’ (2018) 4(1) Journal of Development and Life-Course Criminology 92

Vollmer A, ‘The Criminal Identification Bureau’ (1918) 9(3) Journal of the American Institute of Criminal Law and Criminology 322

– – ‘Revision of the Atcherley Modus Operandi System’ (1919) 10(2) Journal of the American Institute of Criminal Law and Criminology 229

Walker S R, ‘The Police National Computer Records’ (1970) 43 Police Journal 111

Walters I, ‘The police, young offenders and intelligence-led policing’ (2006) 79 (4) Police Journal 305

– – ‘The Policing of Young Offenders’ (2007) 47(4) British Journal of Criminology 635

Williams C, ‘The growth and permanency of Criminal Records, with particular reference to juveniles’ (2011) 84(2) Police Journal 171

Zander M, ‘Arresting someone who is helping the police with their enquiries’ (2010) 174 Criminal Law and Justice Weekly 309

– – ‘The Required Destruction of Custody Photographs’ (2012) 176 Criminal Law and Justice Weekly 489

– – ‘Chief Constables Project, EMSCP and NLEDP Update’ (14 July 2016)

– – ‘Government’s Response to the House of Commons Science and Technology Committee: Biometrics strategy and forensics services’’ (HC 800, 2017 – 19, 5 – I)

– – ‘Report of the Commissioner of the Metropolis for the Year 1961’ (Cmnd 190, HMSO 1961)

– – ‘Sessional Papers, Volume 20’ (HMSO 1961)

– – ‘Sessional Papers, Volume 22’ (HMSO 1920)

ACRO Criminal Records Office, ‘Annual Report 2015 – 16’ (2016)

– – ‘Annual Report 2016 – 17’ (2017)

– – ‘Annual Report 2017 – 18’ (2018)

Appleton R, ‘Pavement Injustice: the tyranny of on-the-spot fines’ (The Manifesto Club 9 February 2012)

Association of Chief Police Officers, ‘Codes of Practice for Police Computer Systems’ (1987)

– – ‘Codes of Practice for Data Protection’ (1995)

– – ‘General Rules for the Criminal Record Weeding on Police Systems’ (November 2000)

– – ‘Retention Guidelines for Nominal Records on the Police National Computer. Incorporating the Step-Down Model’ (March 2006)

– – ‘Data Protection, Manual of Guidance’ (Part II – Audit, 1 July 2007)

– – ‘New Position on the retention of Police National Computer (PNC) Records’ (22 October 2009)

– – ‘ACRO Criminal Records Office, Annual Report 2011 – 12’ (2012)

Association of Chief Police Officers Scotland (ACPOS), ‘Recommended Record Retention Periods’ (February 2011)

– – ‘Recording, Weeding and Retention of Information on Criminal History System – Guidance’ (v.1.0, 23 November 2011)

Audit Commission, ‘Helping with enquiries: tackling crime effectively’ (HMSO 1993)

– – ‘Misspent Youth: Young People and Crime’ (1996)

Bichard M, ‘The Bichard Inquiry Report’ (HC 653, 22 June 2004)

Biometric and Forensic Ethics Group, ‘Response to the Home Office custody images review’ (25 August 2017)

Cannataci J and Caruana M, ‘Recommendation R (87) 15: Twenty-Five years down the line’ (Council of Europe 25 September 2013)

Crown Prosecution Service, ‘Code for Crown Prosecutors – Bail: Opposing Bail, Information for Prosecutors’ (7th edn, 2013)

– – ‘Code for Crown Prosecutors – Disclosure of previous convictions of prosecution witnesses’ (7th edn, 2013)

– – ‘Code for Crown Prosecutors – Jury Vetting: Overview of Jury Checks’ (7th edn, 2013)

– – ‘Code for Crown Prosecutors – Sentencing: evidence of character & antecedents: previous convictions’ (2017)

College of Policing, ‘Management of Police Information’ (3rd edn, 24 October 2014)

Committee of Public Accounts, *The electronic monitoring of adult offenders* (HC 997 2005 – 06, 64 – I)

Constitution Committee, *Surveillance: Citizens and the State* (HL 2008 – 09, 18 – I)

Cooper C and Roe C, ‘An estimate of youth crime in England and Wales’ (Home Office Research Report 64, May 2012)

Couchman H, ‘Why we’re no longer taking part in a consultation on the police’s new super-database’ (Liberty 1 October 2018)

Court J M, ‘Personal Data Protection – the 1984 Act and it’s implications’ (National Computing Centre, 1984)

Crofton W, ‘Convict systems and transportation: a lecture delivered at the Philosophical Institution, Bristol, on the 22nd December 1862’ (LSE Selected Pamphlets 1963)

Data Protection Registrar, ‘The eighth report of the Data Protection Registrar’ (HMSO June 1992)

– – ‘The ninth report of the Data Protection Registrar’ (HMSO June 1993)

Denham E, ‘Speech to the National Police Chiefs’ Council Information Practitioner Event’ (7 June 2017).

Disclosure and Barring Service, ‘Annual Reports and Accounts for the period 1 April 2017 to 31 March 2018’, (HC 1367, 19 July 2018)

– – ‘Annual Reports and Accounts for the period 1 April 2017 to 31 March 2018’ (HC 1367, 19 July 2018)

Earland R, ‘Compliance Strategy for the Police National Computer’ (ACPO 16 February 2000)

Economic and Social Research Council, ‘Review of Socio-Legal Studies: Final Report’ (Swindon, 1994)

European Standing Committee B, ‘Official Report’ (December 1994)

Farrington D P *et al*, ‘Cambridge Study in Delinquent Development; Long-Term Follow-Up’ (Unpublished manuscript. Institute of Criminology, Cambridge University, 1988)

Frances E, ‘Data Protection Bill 2/98, Costs of Implementing the EU Data Protection Directive’ (v.2.0, 29 January 1998)

Gardiner Committee, *Living it Down – the problem of old convictions* (London, Stevens and Sons 1972)

Garside R, ‘Crime, persistent offenders and the justice gap’ (Crime and Society Foundation, October 2004)

Graham J and Bowling B, ‘Young People and Crime’ (Home Officer Research Study 145, 1995)

Hargreaves J, Husband H and Linehan C, ‘Police powers and procedures, England and Wales, year ending 31 March 2017’ (Home Office Statistical Bulletin 20/17, 26 October 2017)

Her Majesty’s Inspectorate of Constabularies, ‘Police National Computer: Data Quality and Timeliness – Report by HM Inspectorate of Constabulary’ (HMIC 2001)

– – ‘Police National Computer: Data Quality and Timeliness – Second Report on the Inspection by HM Inspectorate of Constabulary’ (2002)

– – ‘Metropolitan Police Service, Police National Computer Compliance Report’ (14–18 February 2005)

– – ‘Suffolk Constabulary, Police National Computer Compliance Report’ (6 – 10 June 2005)

– – ‘Hampshire Police, Police National Computer Compliance Report’ (10–13 October 2005)

– – ‘West Mercia Constabulary, Police National Computer Compliance Report’ (12–16 December 2005)

– – ‘Scottish Criminal Record Office. Primary Inspection 2004’ (2005)

– – ‘Northamptonshire Police, Police National Computer Compliance Report’ (19 – 22 February 2007)

– – ‘Police National Computer Compliance Report, 5 – 7 October 2010’ (HMIC January 2011)

– – ‘Mistakes were made: HMIC’s review into allegations and intelligence material concerning Jimmy Saville between 1964 and 2012’ (London, March 2013)

– – Crime Recording in Kent’ (2013)

– – ‘Use of the Police National Computer by non-police organisations: An inspection of the Children and Family Court Advisory and Support Service’ (May 2016)

– – ‘Use of the Police National Computer by non-police organisations: An inspection of Thurrock Council (May 2016)

– – ‘Use of the Police National Computer by non-police organisations: Gangmasters Licencing Authority’ (May 2016)

– – ‘Use of the Police National Computer by non-police organisations: An inspection of the Financial Conduct Authority’ (May 2016)

– – ‘Use of the Police National Computer by non-police organisations: An inspection of Post Office Ltd’ (May 2016)

– – ‘Use of the Police National Computer by non-police organisations: A pilot inspection of Environment Agency’ (May 2016)

– – ‘Use of the Police National Computer by non-police organisations: A pilot inspection of Royal Mail Security Group’ (May 2016)

– – ‘Use of the Police National Computer by non-police organisations: An inspection of Air Traffic Systems Ltd (May 2016)

– – ‘Use of the Police National Computer: An inspection of the ACRO Criminal Records Office’ (April 2017)

Home Affairs Committee (HC 1979 – 80, 1 – I)

– – *Criminal Records* (Cm 285, HC 1989 – 90, 3 – I)

– – *Private Investigators* (HC 100, HC 2012 – 13, 4 – I)

– – *Policing for the Future* (HC 515, HC 2017 – 19, 10 – I)

Home Office Committee, 'The workings of the methods of identification of criminals by measurements and fingerprints, and the administrative arrangements for carrying the system' (1900)

Home Office, 'Report of a Committee appointed by the Secretary of State to inquire into the best means available for identifying Habitual Criminals' (1893 – 94)

– – 'Non-accidental injury to children: the police and case conferences' (HO 179/1967)

– – Police reports of convictions and related information' (HOC 140/1973)

– – 'Privacy Precautions for Computer Systems Handling Personal Data' (1976)

– – *Data Protection: the Government's Proposals for Legislation*, (Cmd 8539, 1982)

– – 'The National Collection of Criminal Records: report of an efficiency scrutiny' (HMSO 1991)

– – 'PHOENIX, Putting you in the picture' (London: Police Department, Science and Technology Group 1995)

– – 'Criminal Justice: The Way Ahead' (HMSO, 2001)

– – 'Final Warning Scheme: guidance for the police and youth offending teams' (Home Office Communication Directorate November 2002)

– – 'Final Warning Scheme' – Guidance for Police' (April 2000)

– – 'Circular 047/2003: Revised Arrangements for Police Checks', Home Office Circular (2003)

– – 'Circular 30/2005: Cautioning of adult offenders' (14 June 2005)

– – 'Circular 14/2006: The Final Warning Scheme' (17 May 2006)

– – 'Prolific and other Priority Offender Programme: five years on: maximising the impact' (HMSO June 2009)

– – 'Police National Computer (PNC) Guidance (version 5.0)' (23 January 2014)

– – 'The PNC User Manual' (v.15.02, December 2015)

– – ‘Modern Crime Prevention Strategy’ (March 2016)

– – ‘Home Office (HO) National Law Enforcement Data Programme (NLEDP) Application Development Service. Tender Application’ (28 October 2016)

– – ‘Review of the use and retention of Custody Images’ (February 2017)

– – ‘Transparency Data: HO Government Major Project Portfolio data, September 2016’ (18 July 2017)

– – ‘National DNA Database statistics, Q4 2017 – 18’ (23 May 2018)

– – ‘Statistical News Release: Crime Outcomes in England and Wales, year ending March 2018’ (19 July 2018)

– – ‘National Law Enforcement Data Programme: Law Enforcement Data Service – Privacy Impact Assessment Report’ (July 2018)

– – ‘Impact Assessment: Third Country Nationals and the European Criminal Records Information System’ (10 August 2018)

HM Government, ‘Working Together to Safeguard Children’ (July 2018)

Independent Police Complaints Commission, ‘Statistics for England and Wales 2016/17’ (2017)

Information Commissioner’s Office, ‘Annual Report 2007/08’ (HC 670, 2008)

– – ‘Police cases: ICO’s response to the Court of Appeal’s judgment’ (Press Release 13 November 2009)

– – ‘Information Commissioner’s Annual Report 2009/10’ (HC 220, 2010)

Justice Sub-Committee on Policing, ‘Police Scotland’s Digital Data and IT Strategy: Evidence Session’ (Written Submission: Police Scotland, Scottish Parliament, 10 May 2018)

Kershaw C, Goodman J, and White S, ‘Reconvictions of Offenders Sentenced or Discharged from Prison in 1995, England and Wales’ (HOSB 19/99, 1999)

Law Commission, *Evidence of Bad Character in Criminal Proceedings* (Law Com No 273, 2001)

– – *Criminal Records Disclosure: Non-Filterable Offences* (Law Com. No.371, 2017)

Liberty, ‘Liberty’s response to the Home Office White Paper ‘Justice for All’’ (October 2000)

Lindop N, *Report of the Committee on Data Protection* (Cmd 7341, 1978)

Judge I, 'Summary Justice In and Out of Court' (John Harris Memorial Lecture, Draper's Hall, London, 7 July 2011)

MacGregor A, 'Annual Report: Commissioner for the retention and use of biometric material' (HMSO 10 November 2014)

MacGregor A, 'Commissioner for the retention and use of Biometric Material – Annual Report 2014' (The Office of the Biometric Commissioner, November 2014)

Mason S, 'A balanced approach: safeguarding the public through the fair and proportionate use of accurate criminal record information' (HO 01671 G, March 2010)

– – 'A common sense approach: a review of the criminal record regime in England and Wales (Report on Phase Two)' (Home Office 30 November 2011)

McNeil F *et al*, 'How and why people stop offending: discovering desistance' (University of Glasgow Institute for Research and Innovation in Social Services, 2012)

Metropolitan Police: 'Criminal Records Office: Habitual Criminal Registers and Miscellaneous Papers' (MEPO 6, 1834 – 1959)

– – 'Catching Thieves on Paper: History and Purpose of the Criminal Record Office and the Police Gazette and it's supplements' (MEPO 8/42 1936)

Ministry of Justice, 'Operation of the Police National Computer' (1 March 1999)

– – 'Conviction histories of Offenders between the ages of 10 and 52. England and Wales' (15 July 2010)

– – 'Youth Crime: Young People aged 10 – 17 receiving their first reprimand, warning or conviction, 2000–1 to 2009–10' (14 October 2010)

– – 'The Youth Justice System in England and Wales': reducing offending by young people' (HC 663, 10 December 2010)

– – 'Criminal statistics annual report: chapter 2, Penalty notices for disorder' (4 May 2012)

– – '2012 Compendium of re-offending statistics and analysis' (12 July 2012)

– – 'The Criminal Injuries Compensation Scheme 2012' (The Stationery Office 2012)

– – 'Code of Practice for Adult Conditional Cautions – Part 3 of the Criminal Justice Act 2003' (January 2013)

– – 'Criminal justice statistics quarterly: December 2012' (30 May 2013)

– – ‘Criminal Justice Statistics, Quarterly Update to December 2012, England and Wales’ (30 May 2013)

– – ‘Guidance on the Rehabilitation of Offenders Act 1974’ (4 March 2014)

– – ‘Penalty Notices for Disorder (PNDs)’ (24 June 2014)

– – ‘Simple Cautions for Adult Offenders: guidance for police officers and Crown Prosecutors’ (13 April 2015)

– – ‘Criminal Justice Statistics quarterly, England and Wales, September 2016 to September 2017’ (18 February 2018)

– – ‘Criminal Justice Statistics Quarterly, Out of Court Disposals 2007 – 2017, Pivot Analytical Tool for England and Wales’ (17 May 2018)

– – ‘Criminal Justice Statistics, Quarterly: Out of Court Disposals Tools (December 2017)’ (17 May 2018)

– – ‘Proven Re-offending statistics Quarterly Bulletin, January 2017 to March 2017’ (31 January 2019)

– – ‘Youth Justice Statistics 2017/18 England and Wales’ (31 January 2019)

Multi-Agency Public Protection Arrangements, ‘Disclosure of Information Leaflet’ (2008)

Ministry of Justice, ‘Multi-Agency Public Protection Arrangements, Annual Report 2016/17 (Office for National Statistics October 2017)

Murray P J, ‘Not so bad as they seem: The Transportation, ticket-of-leave, and penal servitude questions, plainly stated, and argued on facts and figures, with come observations on the principles of prevention, in a letter addressed to Matthew Devenport Hill’ (Knowsley Pamphlet Collection 1857)

National Centre for Policing Excellence, ‘Code of Practice on the Management of Police Information’ (July 2005)

National Police Chief’s Council and the Home Office, ‘National DNA Database Strategy Board Annual Report 2017/18’ (APS Group, HMSO, February 2018)

National Police Chief’s Council, ‘Deletion of Records from Police National Systems (PNC/NDNAD/IDENT1)’ (v.1.1, 19 March 2015)

– – ‘Deletion of Records from National Police Systems’ (2015)

– – ‘ACRO Criminal Records Office, Step Down Model, Filtering of offences for Certificates of Convictions’ (5 January 2018)

– – ‘Deletion of records from national police systems (PNC/NDNAD/IDENT1)’ (18 October 2018)

National Policing Improvement Agency, ‘Memorandum by the National Policing Improvement Agency’ (NPIA December 2007)

– – ‘Guidance on the Management of Police Information’ (2nd edn, 2010)

National Statistics (Scotland), ’Recorded Crime in Scotland, 2017 – 18’ (25 September 2018)

Norris P and Palmer J, ‘Comparability of the Crime Surveys in the UK: a comparison of victimisation and technical details’ (Scottish Centre for Crime and Justice Research 2010)

Nuttall C, Goldblatt P and Lewis C, ‘Reducing Offending: An assessment of Research Evidence on ways of dealing with Offending Behaviour’ (Home Office Research, Development and Statistics Directorate, 1998)

Office for National Statistics, ‘Crime in England and Wales, year ending December 2017’ (28 April 2018)

Police Information Technology Organisation, ‘A review of Phoenix input standards and data quality’ (1996)

Police Scotland, ‘Recording, Weeding and Retention of Information on Criminal History System – Guidance (v.2.0, 6 June 2013)

– – ‘Recording, Weeding and Retention of Information on Criminal History System – Guidance’ (v.4.0, 2 August 2018)

Povey K, ‘On the Record: Thematic Inspection Report on police crime recording, the Police National Computer and Phoenix Intelligence System data quality’ (HM Inspectorate of Constabulary July 2000)

Report of the Working Group on the Recording and Weeding Policy for the Criminal History System (Scottish Criminal Record Office October 2004)

Russell J, ‘Home Office Police Research Group Special Interest Paper 11 – Phoenix data quality’ (HC Library Dep 98/183, 9 April 1998)

Safer Scotland, ‘Discussion paper on the Rehabilitation of Offenders Act 1974’ (APS Group Scotland, August 2013)

Savage N and Edwards C, ‘A guide to the Data Protection Act 1984’ (Financial Training Publications 1985)

Science and Technology Committee, *Current and future use of biometric data and technologies* (HC 734, 2014 – 15, 6 – I)

– – *Biometrics strategy and forensics services* (HC 800, 2017 – 19, 5 – I)

Scottish Government, ‘Discussion Paper on the Rehabilitation of Offenders Act 1974’ (27 August 2013)

– – ‘Criminal Proceedings in Scotland 2017 – 18’ (National Statistics, 2018)

Scottish Law Commission, *Report on Similar Fact Evidence and the Moorov Doctrine* (Scot Law. Comm 229, 2012)

Scottish Office (Police), Circular No.4 of 1989

Select Committee on Home Affairs, *Criminal Records Bureau* (HC 227, 2000 – 1, 2-I)

Social Exclusions Unit, ‘Reducing re-offending by ex-prisoners’ (The Office of the Deputy Prime Minister July 2002)

Steer D, ‘Recorded Convictions’ (1971) University of Oxford Penal Research Unit

The Information Commissioner’s Office, ‘Guide to the Data Protection Regulation (GDPR)’ (4 June 2018)

United Kingdom Security Vetting, ‘National Security Vetting: advice if you are being vetted by us’ (February 2018)

Wakefield & District Safeguarding Board, ‘protocol for police attendance at Initial Child Protection Conferences’ (October 2015)

Wiles P, ‘Response to the Home Office review of the retention and use of custody images’ (17 March 2017)

– – Annual Report: Commissioner for the retention and use of biometric material, (HMSO March 2018)

Willink H, *Royal Commission on the Police, Final Report* (Cmd 1728, 1962)

Wood E, ‘Research Paper 98/48’ (HC Library, 17 April 1998)

Younger K, *Report on the committee on privacy* (Cmd 5012, 1972)

Tertiary sources (including news media reports)

– – ‘Baffling case of gliding eyeball’ *The Daily Mirror* (London, 22 April 1993)

– – ‘Branded a thief and barred from a job’ *The Daily Record* (Glasgow, 20 June 1995)

– – ‘Court of Appeal overturns sentence on West Midlands police officer and imposes prison term’ *The Birmingham Post* (Birmingham, 16 October 2009)

– – ‘Crime figures: Violent Crime recorded by polices rises by 19%’ *The BBC* (London, 24 January 2019)

– – ‘Criminal records must be erased’ *The BBC* (London, 22 July 2008)

– – ‘Data Protection guidance pledge’ *The BBC* (London, 14 January 2004)

– – ‘Ex-West Midlands Police officer jailed in drugs charge’ *The BBC* (London, 24 April 2015)

– – ‘Former police private eyes jailed’ *The BBC* (London, 10 October 2007)

– – ‘Home Office appoints crime data adviser’, *The Guardian* (London, 7 September 2009)

– – ‘Juries learn sex offenders’ past’ *The BBC* (London, 25 October 2004)

– – ‘Leak verdict’ *The Times* (London, 27 February 1988)

– – ‘Officer says misuse is falling’ *The Times* (London, 8 May 1990)

– – ‘Police attacked over Huntley data’ *The BBC* (London, 24 February 2004)

– – ‘Police can keep records of minor convictions for 100 years’ *The Telegraph* (London, 19 October 2009)

– – ‘Police find a Catch-22 for data victim’ *The Guardian* (London, 8 October 1986)

– – ‘Police leaks justified’ *The Times* (London, 26 February 1998)

– – ‘Police pair jailed on files leak’ *Birmingham Evening Mail* (Birmingham, 23 February 1999)

– – ‘Police records ‘were leaked’’ *The Guardian* (London, 24 February 1998)

– – ‘Police told to delete old criminal records’ *The Guardian* (London, 1 November 2007)

– – ‘Police warned twice over Huntley’ *The BBC* (London, 25 March 2004)

– – ‘Police win appeal to keep minor convictions on file’ *The Guardian* (London, 19 October 2009)

– – ‘Police win data deletion appeal’ *The BBC* (London, 19 October 2009)

– – ‘Policeman jailed’ *The Times* (London, 5 July 1997)

– – ‘Policemen guilty of conspiracy over computer information’ *The Independent* (London, 3 February 1989)

– – ‘Q & A, Data Protection and the Police’ *The Guardian* (London, 18 December 2003)

– – ‘Scots feel safer than ever before’ *The BBC* (London, 27 March 2018)

– – ‘Scottish homicides at lowest level since 1976’ *The BBC* (London, 30 October 2018)

– – ‘Shoplifters to get fine let-off’ *BBC* (London, 30 May 2007)

– – ‘UK criminal vetting errors double’ *The BBC* (London, 3 August 2009)

– – ‘UK news in brief: clean slate for petty offenders’ *The Guardian* (London, 15 March 1985)

– – ‘Women in wrong identity blinder’ *The BBC* (London, 25 June 2007)

Agerholm H, ‘Rape victims with records of minor offences regularly denied compensation’ *The Independent* (London, 5 April 2017)

Anderson R and Stoneman R, ‘GlobalData on Home Office funding for the law enforcement data programme’ *Government Computing* (London, 23 November 2018)

Coleman C, ‘Police facial recognition surveillance court case starts’ *The BBC* (London, 21 May 2019)

Cowdry Q and Souster M, ‘Separate agency ‘would ensure accurate records’ *The Times* (London, 8 May 1990)

Crossland S, ‘A nation without secrets’ *The Sunday Times* (London, 16 July 1989)

Curry L, ‘A stickler for our privacy: the new Data Protection Registrar is taking on banks’, *The Independent* (London, 19 September 1994)

Deane A, ‘A criminal ruling on criminal records’ *Big Brother Watch* (19 October 2009)

Dyer C, ‘Criminal record errors causing lighter sentences’ *The Guardian* (London, 3 March 1994)

– – ‘Juries may be told of previous convictions’ *The Guardian* (London, 26 October 2004)

Evans P and Dawe T, ‘Review of police security’ *The Times* (London, 4 February 1989)

Finnigan L,' Litter Wardens suspended after woman fined £80 for feeding ducks' *The Telegraph* (London, 30 September 2016)

Gibb F, 'Sentences based on inaccurate criminal records, MP's told' *The Times* (London, 22 February 1990)

Hall K, 'Police create mega crime database to rule them all. Is *your* numberplate in it? Could be' *The Register* (London, 23 March 2016)

Hope C, 'Hundreds of innocent people 'wrongly branded criminals' by CRB checks' *The Telegraph* (London, 4 July 2008)

Hughes M, 'Now data watchdog fears for loses in the numbers game' *The Guardian* (London, 22 July 1990)

Hymas C, 'Criminals to be handed clean slate under Sajid Javid plan to wipe minor offences when applying for jobs' *The Telegraph* (London, 16 April 2019)

Large P, 'Data error complaints double' *The Guardian* (London, 2 March 1990)

Leask D, 'Police investigate tough drugs policy' *The Herald* (Glasgow, 8 April 2008)

Leigh D and Davies N, 'Evidence of illegal data checks on Gordon Brown buried by 2005 ruling', *The Guardian* (London, 11 July 2011)

Leigh D, 'Police give computer secrets out', *The Observer* (Manchester, 4 October 1981)

Leppard D, Burke J and Kelsey T, 'Corrupt police sell secrets in Yard scandal' *The Sunday Times* (London, 24 August 1997)

Lewis J, 'Hundreds of police officers caught illegally accessing records computer' *The Telegraph* (London, 20 August 2011)

McGivern M, 'Cops hit man with £50 fine – for dropping £10 note in the street' *Daily Record* (Glasgow, 11 June 2009)

McSmith A, 'No retreat on Tories' cannabis hard-line' *The Telegraph* (London, 7 October 2000)

Meikle J, 'Police may have to destroy photos of innocent people after court ruling' *The Guardian* (London, 22 June 2012)

O'Neill S and Stokes P, 'Police chief faces axe for deleting Huntley records' *The Telegraph* (London, 19 December 2003)

Oates J, 'Police told: delete old criminal records' *The Register* (22 July 2008)

Rozenberg J, ‘Juries will be told of previous convictions’ *The Telegraph* (London, 26 October 2004)

Simons M, ‘Errors rife in police data file’ *Computer Weekly* (London, April 2000)

Souster M, ‘Innocent man in case of mistaken identity’ *The Times* (London, 8 May 1990)

Stern C, ‘Crime files are stolen from national computer’ *Mail on Sunday* (London, 14 August 1994)

Topping A and Quinn B; ‘Charles Saatchi: accepting police caution was better than the alternative’ *The Guardian* (London, 18 June 2013)

Weaver M, ‘Homicides in England and Wales rise by 14%’ *The Guardian* (London, 24 January 2019)

Whitehead T, ‘Thousands wrongly labelled as criminals’ *The Telegraph* (London, 2 February 2012)

– – ‘Police breach human rights by keeping photos of innocent’ *The Telegrap*h (London, 22 June 2012)

Woods D, ‘Court ruling gives employers access to employee’s criminal records’ *Human Resources Magazine* (London, 20 October 2009)

Wright R, ‘UK fears over rising crime muddied by contradictory statistics’ *The Financial Times* (London, 8 August 2018)

Websites and other online sources

'DBS checks: guidance for employers' (DBS Online, 3 April 2019) <https://www.gov.uk/guidance/dbs-check-requests-guidance-for-employers#overview> accessed 16 April 2019

'FOI Release. Nominal Criminal Records on the Police National Computer' (Home Office FOI release 33517, 21 January 2015) <https://www.gov.uk/government/publications/nominal-criminal-records-on-the-police-national-computer> accessed 15 May 2019

'FOI Request. Officers and Staff illegally accessing PNC' (Gloucestershire Constabulary, 9 February 2017) <https://www.gloucestershire.police.uk/more-on-us/freedom-of-information/disclosure-log/operational-policing/officers-and-staff-illegally-accessing-pnc/> accessed 29 May 2019

'Illegal access to the PNC' (Request 0051 – 17, British Transport Police Online Log February 2017) <http://www.btp.police.uk/about_us/your_right_to_information/publication_scheme/disclosure_log/complaints_and_discipline.aspx> accessed 26 April 2019

'PCL Loses Criminal Records Job' (*Computing Online*, 2 October 1996) <https://www.computing.co.uk/ctg/news/1835451/pcl-loses-criminal-records-job> accessed 8 April 2019

'Police National Computer Services: Requesting PNC services for your organisation' (ACRO Criminal Record Office, 2018) <https://www.acro.police.uk/acro_std.aspx?id=197> accessed 21 August 2018

Home Office, 'FOI Release. Number of nominal records on the Police National Computer' (FOI ref 44921, *What Do They Know?* 27 October 2017). <https://www.whatdotheyknow.com/request/number_of_nominal_records_on_the#incoming-1060100> accessed 15 May 2019

Home Office, 'FOI Request. Agencies with PNC access' (FOI Ref 37592, *What Do They Know?* 22 November 2015) <https://www.whatdotheyknow.com/request/agencies_with_pnc_access#incoming-753180> accessed 16 May 2019

Home Office, 'FOI Request. Collection of historic microfiche criminal records' (FOI Case Ref: 49433 *What Do They Know?* 17 July 2018)

<https://www.whatdotheyknow.com/request/collection_of_historic_microfich#incoming-1205670> accessed 8 April 2019

Home Office, 'FOI Request. Number of people with criminal convictions on the PNC' (FOI Reference CR33517, *What Do They Know?* 13 November 2014) <https://www.whatdotheyknow.com/request/number_of_people_with_criminal_c#incoming-595350> accessed 7 August 2018

Home Office, 'FOI Request. Request for information regarding access to the Police National Computer' (FOI Case Ref: 49917 *What do they Know?* 21 August 2018) <https://www.whatdotheyknow.com/request/request_for_information_regardin_120#incoming-1236064> accessed 21 August 2018

Home Office, 'Freedom of Information request. PNC Access by Prisons' (FOI/61065 *What Do They Know?,* 2 September 2009) <https://www.whatdotheyknow.com/request/pnc_access_by_prisons#comment-29988> accessed 22 August 2018

Hyde J, 'Court overturns legal aid denial in wrongful arrest case' (*Law Society Gazette,* 13 November 2014) <https://www.lawgazette.co.uk/law/court-overturns-legal-aid-denial-in-wrongful-arrest-case/5045066.article> accessed 20 May 2019

O'Connor T, 'Does a recent decision mean some people will never escape past convictions?' (5 November 2009) Law Society Gazette <https://www.lawgazette.co.uk/law/-does-a-recent-decision-mean-some-people-will-never-escape-past-convictions/52936.article > accessed 23 May 2019

The Information Commissioner, 'FOI Request. Data relating to enforcement notices issued to police forces in respect of the nominal index of the PNC' (Case Ref: IRQ0772426 *What Do They Know?,* 1 August 2018) <https://www.whatdotheyknow.com/request/data_relating_to_enforcement_not#incoming-1221131> accessed 1 August 2018

The Information Commissioner, 'FOI Request. Data relating to enforcement notices issued to police forces in respect of the nominal index of the PNC' (Case Ref No. IRQ0772426, *What Do They Know?* 1 August 2018) <https://www.whatdotheyknow.com/request/data_relating_to_enforcement_not#describe_state_form_1> accessed 1 August 2018

The Information Commissioner, 'FOI Request. Information relating to enforcement notices issued to the National Identification Bureau' (Case Ref: IRQ0772425, *What Do They*

Know? 1 August 2018).
<https://www.whatdotheyknow.com/request/information_relating_to_enforcem>
accessed 21 October 2018