



Renaud, Karen, Bongiovanni, Ivano, Wilford, Sara and Irons, Alastair (2021) PRECEPT-4-Justice: A Bias-Neutralising Framework for Digital Forensics Investigations. Science and Justice. ISSN 1355-0306

Downloaded from: <http://sure.sunderland.ac.uk/id/eprint/13593/>

Usage guidelines

Please refer to the usage guidelines at <http://sure.sunderland.ac.uk/policies.html> or alternatively contact sure@sunderland.ac.uk.

Journal Pre-proofs

Short Communication

PRECEPT-4-Justice: A Bias-Neutralising Framework for Digital Forensics Investigations

Karen Renaud, Ivano Bongiovanni, Sara Wilford, Alastair Irons

PII: S1355-0306(21)00068-X
DOI: <https://doi.org/10.1016/j.scijus.2021.06.003>
Reference: SCIJUS 958



To appear in: *Science & Justice*

Received Date: 19 February 2021
Revised Date: 26 April 2021
Accepted Date: 6 June 2021

Please cite this article as: K. Renaud, I. Bongiovanni, S. Wilford, A. Irons, PRECEPT-4-Justice: A Bias-Neutralising Framework for Digital Forensics Investigations, *Science & Justice* (2021), doi: <https://doi.org/10.1016/j.scijus.2021.06.003>

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

PRECEPT-4-Justice: A Bias-Neutralising Framework for Digital Forensics Investigations

Anon

Abstract

Software invisibly permeates our everyday lives: operating devices in our physical world (traffic lights and cars), effecting our business transactions and powering the vast World Wide Web. We have come to rely on such software to work correctly and efficiently. The generally accepted narrative is that any software errors that *do* occur can be traced back to a human operator’s mistakes. Software engineers know that this is merely a comforting illusion. The software, hardware and communication infrastructure can all introduce errors, which are often challenging to isolate and correct. Anomalies that manifest are certainly not always due to an operator’s actions. When the general public and the courts believe the opposite, it is entirely possible for some hapless innocent individual to be blamed for anomalies and discrepancies whose actual source is a software malfunction. This is what occurred in the Post Office Horizon IT case, where unquestioning belief in the veracity of software-generated evidence led to a decade of wrongful convictions. We will use this case as a vehicle to demonstrate the way biases can influence investigations, and to inform the development of a framework to guide and inform objective digital forensics investigations. This framework, if used, could go some way towards neutralising biases and preventing similar miscarriages of justice in the future.

1 Introduction

Sometimes the justice system gets things wrong. In May 2004, US citizen Brandon Mayfield was wrongfully arrested on suspicion of being the perpetrator of the 2004 Madrid train bombings based on automated fingerprint correlation, which is thought to have swung the case [28]. In another case, Christina Allcock appealed and successfully had her conviction overturned, because the appeal judge ruled that Facebook messages used during her trial lacked sufficient evidentiary foundation [78]. In both these cases, unquestioning faith in the correctness of software-generated evidence led to unsafe convictions. In fact, the presumption that computers work correctly is “*frustrating [and] deeply flawed*” [16], when in reality software errors are common, and can potentially cause unpredictable [21] or destructive behaviours [75]. The ramifications, for both the accusers and the unjustly convicted, are momentous.

Justice is a Universal Human Right [116], and we expect criminal prosecutions to be based on solid evidence, resulting from investigations carried out with due diligence. The concept of reasonable doubt in criminal

prosecutions requires all evidence to be weighed objectively [71]. When software-generated evidence is used in court, circumstantial evidence and contextual information must reinforce and confirm any initial conclusions drawn from an analysis of such digital evidence. Marshall *et al.* [64, p.19] argue that when computer-generated evidence is used, that it must be confirmed that: “*at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents.*”

One of the longest running miscarriages of justice in modern Britain came to a head during the Post Office Horizon IT trial of 2019 [119, 80]. The strong influence of unverified software-generated evidence in the Post Office Horizon IT Case [76] provides us with a case study that we can use to demonstrate how biases can influence investigations. The courts have already ruled on this case and it is not our intention to identify culprits. We use this case solely as a vehicle to demonstrate the impact of biases on digital investigations, and to help us to formulate a framework for mitigating these.

To prevent miscarriages of justice, the best place to intervene is during investigations i.e. when evidence is being gathered and analysed [85]. Hence, our aim in this research is a constructive one, namely “*in investigations where software-generated evidence is involved*, identify, expose, and explain disinformation where and when it occurs using open source research” (adapted from the Atlantic Council’s Digital Forensics Lab’s aim¹ – our addition in italics).

To achieve our goal, we have derived a framework, which we call PRECEPT-4-Justice, designed specifically to help investigators maintain objectivity during investigations.

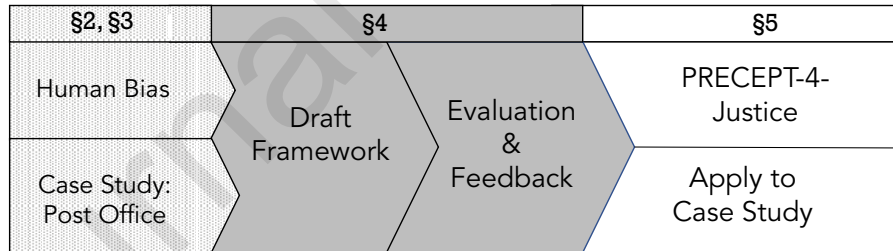


Figure 1: The Research Reported in this Paper (with Section numbers)

The research process is depicted in Figure 1, including stages, and the sections where each stage is reported on. We commence by identifying the range of biases that could lead to subjectivity during investigations (Section 2). We then report on our analysis of the Post Office Horizon IT case with a view to understanding the chain of events that led to it, and the root-cause dynamics that contributed to it (Section 3). Having identified the pertinent biases and root causes, we proceeded to formulate an intervention in the form of a framework which can inform and guide future investigations to minimise the impact of human bias and subjectivity in investigations that rely on software-generated or -derived evidence (Section 4). Section 5 presents the final

¹<https://www.digitalsherlocks.org/about>

framework, discusses the limitations and suggests future work, and Section 6 concludes.

2 Bias in Investigations

Courts should be able to rely on the integrity and unbiased nature of investigation outcomes. It is important to ensure that any evidence presented to courts is trustworthy, unbiased and the outcome of an objective and thorough investigation. Indeed, the Forensic Science Regulator [39] mentions the need for objectivity five times in their code of practice. Item 2 in their Code of Conduct states: “*Act with honesty, integrity, objectivity and impartiality, and declare at the earliest opportunity any personal, business and/or financial interest that could be perceived as a conflict of interest*”. We sought to identify the best way of assuring that investigations are carried out in line with this code of practice.

2.1 Human Bias as a Confounding Factor

For the purposes of this discussion, we assume that investigators are honest and well-intentioned, and that they are aware of the code of conduct laid down by the Forensic Science Regulator [39]. Even so, investigations may still lead to flawed conclusions. The source, in many cases, is human bias, which might influence investigators without their even being aware of it. Such biases can introduce subjectivity into an investigation, where the gold standard would be for investigators to separate judgements from evaluations [70].

Within the legal system, biases inevitably reach all the way to the courts and impact the judiciary, since everyone is human and thus subject to bias. Nakhaeizadeh *et al.* [70, p. 208] argue that biases might impact an investigator’s activities throughout the investigation: (1) while collecting data, (2) carrying out the analysis, and then (3) interpreting it. This pervasive influence of bias across the investigation process is also highlighted by a number of other researchers [41, 53, 2, 26]. The next section offers a brief overview of the different types of biases.

2.2 Investigation-Relevant Human Bias

Sunde and Dror [110] enumerate a range of bias types that can influence digital forensics investigations. MacFarlane [63] and Sorochoam [107] review a number of wrongful convictions, and provide explanations for these. We will briefly review the biases and factors they mention here (we provide examples from well-known non-digital forensics cases because the biases are investigator related and not domain specific).

Bias 1: Confirmation Bias: This phenomenon is also referred to as anchoring, availability bias or tunnel vision. Nickerson [72, p. 175] defines confirmation bias as ‘*the seeking or interpreting of evidence in ways that are partial to existing beliefs, expectations, or a hypothesis in hand*’, and it may easily lead to miscarriages of justice [89, 40]. Boring [13] explains how ‘*expectations shape perception*’ in that people will generally see

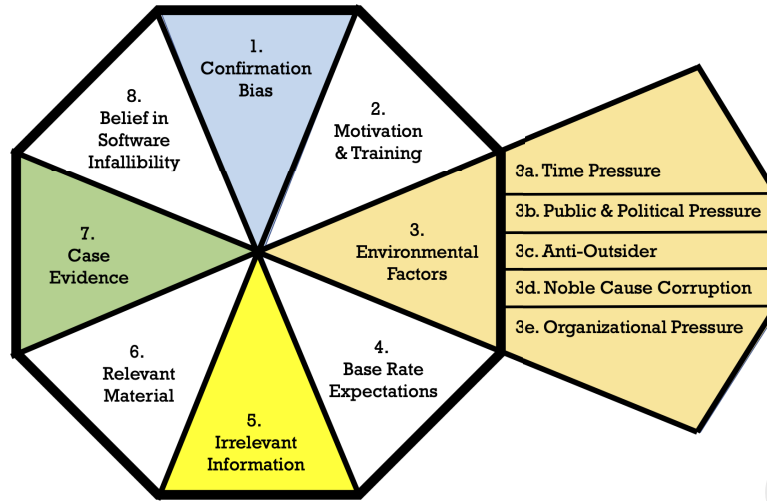


Figure 2: Eight Investigation-Relevant Biases

what they expect to see. Often, confirmation bias is a personal judgement, based on previous experiences and expectations. In cases with a high media interest, a profile of the perpetrator created by the media, could lead to someone who merely fits the profile, being accused. Further, Woffind [124] quotes lawyer Tanner Bolt, who said: “*Most cops, they decide on a suspect and they don’t want to veer at all.*” This is human nature, not specific to police investigations.[72]. Gould *et al.* [44] explain that investigators, if they allow themselves to be influenced by bias in the initial stages of an investigation, then implicitly move from ‘inspection’ to ‘selling’ mode, discarding any evidence they encounter which would negate their existing stance. Garrett [43] confirms this by dissecting a number of cases where poor forensics evidence was used to convict people who were subsequently exonerated. Many of these occurred because forensics investigators appeared to have been looking for confirmatory evidence and did not entertain alternative explanations.

Example Cases: The Dutch Schiedam Park murder [96], where tunnel vision compromised an investigation, subsequently led to an extensive review of police procedures.

Bias 2: Motivation & Training: Investigations are inevitably influenced by investigators’ prejudices, preferences and bias. Sunde and Dror refer to ‘*pre-existing attitudes and with whom the individual identifies, might also sway observations and conclusions*’ [110, p.104]. Moreover, digital forensics investigators are often employed by the prosecution, or defence, and this is likely to bias their investigations and eventual conclusions [100]. People are generally unaware of their biases in this respect [30].

With respect to training, Sunde [110] interviewed digital forensic professionals and found that they had little formal knowledge of bias or indeed the relevant countermeasures they could take to neutralise these. Their educational background or professional training had not covered this. Without awareness of their own biases, it is likely that these would influence investigations [86, 126]. The Canadian FPT Heads of Prosecutions Committee

[40] provides a number of suggestions for training forensics investigators, including “*presentation of case studies of wrongful convictions and lessons learned*” and “*regular newsletters on miscarriage of justice issues*”. These can serve to make investigators aware of their unconscious biases, which is a first step towards neutralising them [74].

Bias 3: Environmental Factors: These are mentioned by [95] and also by [110] and include a variety of factors:

3a. Time Pressure: When investigators are under time pressures, the drive to catch and convict the criminals quickly can become overwhelming. They might well reach for the first feasible conclusion [70] meaning that conclusions are drawn based on convenience and speed rather than on the available evidence.

Example Case: The “Guildford Four” case in the UK in 1975 led to four people being convicted of planting bombs in Guildford and Woolwich. There was public outrage and anger due to recent bombings and resulting deaths. The police were under tremendous pressure to find the culprits as quickly as possible. The resulting unsafe convictions were eventually overturned 15 years later [117].

3b. Public and Political Pressure: Macfarlane [63] highlights the impact this can have on investigations, especially where the crime has been particularly shocking [40]. Borchard [12, p. 372] says “*Public opinion is often as much to blame as the prosecutor or other circumstances for miscarriages of justice*”. A crime that outrages the population could be a factor in a biased investigation and a consequent miscarriage of justice (e.g., [105]). This kind of external pressure can be difficult to resist, particularly if an individual has been identified by the media as being a potential perpetrator.

Example Case: A case where political pressure was applied occurred during World War II, when a US court upheld a decision to inter Japanese-American citizens [112].

3c. Anti-Outsider: When a suspect is perceived to be an outsider, the investigator might be more likely to look for evidence to incriminate them [63]. This can result in people being targeted as potential criminals based on prejudices such as race, gender or socio-economic status. The on-going impact of this form of bias can be self-perpetuating, as more people are targeted and, in some cases, convicted due to anti-outsider bias. The subsequent higher number of previous convictions from such groups leads to further assumptions of guilt for members of these groups.

Example Case: In 1903, George Edalji was assumed to be guilty of a series of crimes in his village, seemingly due to his Indian heritage [111]. Arthur Conan Doyle became involved at Edalji’s request, and proved his innocence.

3d. Noble Cause Corruption: Investigators may personally consider the end to justify the means because one particular outcome is perceived, by them, to be in the public interest [63], or even potentially career and personal reputation enhancing should they solve the crime quickly. This can lead to potential miscarriages of

justice through scapegoating, making an example case or closing a case without sufficient in-depth investigation when it has seen particular public or media pressure.

Example Case: The wrongful conviction of Miss Icie Sands in Harlem, NY is a case in point [15]. Police Officers arrested her for vagrancy because they wanted to “clean up prostitution in New York”.

3e. Organisational Pressure: This occurs when an investigator is operating within an environment that encourages “*acceptance of pre-analysis and pre-decision-making information that may be irrelevant, speculative, incomplete, out of context, or simply wrong*” [63, p.6]. An established organisational culture can lead to pressure on individuals to focus on following organisational expectations rather than professional standards. Where investigations are internal, a pre-existing bias for or against an employee might influence assumptions of guilt if a complaint is made.

Example Case: Danny Major was a police officer who was accused of assaulting a teenager in custody [90]. An internal investigation found him guilty but twelve years later he was exonerated, and the investigators criticised for their “*poor investigative rigour and a mindset that could be described as “verification bias”*”. This can also work in the opposite direction. In 2009, a policeman called Simon Harwood hit Mr Ian Tomlinson from behind and shoved him to the ground. Mr Tomlinson died within minutes from abdominal bleeding [6]. An internal investigation ruled that Mr Tomlinson had died of natural causes. Video footage released by the public eventually led to a court case and PC Harwood was found guilty of gross misconduct [5].

Bias 4: Base Rate Expectations: Base rate expectations from previous cases can influence new investigations [95]. Kassir *et al.* [53] find no evidence for investigatory experience helping to neutralise propensity for bias. While previous experience can be helpful in avoiding blind alleys, it may also lead to inaccurate interpretations due to the influence of previous findings. Therefore, the experience that aids an investigator to make appropriate decisions, can equally lead to the wrong conclusions being drawn. Further, organisational base rate expectations resulting from many such assumptions being made, may result in unsafe precedents which are then encouraged by organisational pressure. For example, a police officer might have successfully investigated a similar crime and then unwittingly expect the current crime to pan out in a similar way. In essence, they are being influenced by their own personal experience, and may also set an organisational precedent for dealing with certain cases in a particular way by other investigators.

Example Case: Consider the case of Barry George, who was convicted for the murder of British journalist Jill Dando outside her home on 26 April 1999. George was convicted and given a life sentence on 2 July 2001, despite the flimsiness of the circumstantial evidence against him [104]. It is possible that his past history of stalking women had created a base rate expectation in the investigators’ minds [4]. Over time, this kind of confirmation bias can create an institutionalised base rate expectation, whereby certain profiles are seen as a ‘safe bet’ for securing convictions. Barry George was subsequently retried and acquitted in August 2008 [4].

Bias 5: Irrelevant Case Information: Contextual information is potentially biasing throughout an investigation [68]. Cooper and Meterko [20], in their systematic review of confirmation bias in forensic science, found that investigators might easily set too much store by information that *appears* influential, and that this could easily set them on the wrong path if that information is unreliable. Furthermore, the communication pathways in digital forensics often include close cooperation, including access to irrelevant information, leading to further bias in the investigation [24].

As more information and more people become involved in the case, and are influenced by that information, and as they then influence others, this increases the levels of bias so that it *‘gathers more momentum as more people are affected by it and then affect others, hence the snowball effect’* [110, p.105]. During digital forensic investigations, the investigator might also have been part of the data collection team, thereby collecting contextual information, discussing the case, speculating and exacerbating the bias. However, due to the size and complexity of digital investigations, choices about what to search for, as well as how, require some knowledge of the context to narrow down the search. It is challenging and may be impossible for investigators in such situations not to be exposed to irrelevant yet influential information.

Example Case: The case of Paul and Elaine Gait is a case in point. In December 2018, a number of flights were grounded at Gatwick airport in London because of a mysterious drone that was observed flying nearby. Based on a Facebook page which showed that Paul owned a remote controlled helicopter, both were arrested and detained for 36 hours [123]. This occurred despite the fact that they were able to prove that they were at work when the drone was observed flying and neither owned a drone. The police force was fined £200 000 for wrongful arrest two years later [108].

Bias 6: Reference Material: Reference material is usually used to compare previous and current data to find a match, such as through fingerprinting or DNA analysis. However, in digital forensics investigations it may be necessary for the investigator to be provided access to information for cross-checking. Where this information contains contextual information, the reference material *‘constitutes a target driven bias where it, rather than the actual evidence, is guiding the cognitive process’* [110, p.106].

Example Case: An example is the case of Brandon Mayfield [28] where access to his fingerprints was provided too soon in the investigation, which homed the investigation onto him, whereas he was actually innocent of the crime.

Bias 7: Case Evidence: The case evidence itself can be a source of bias, from the personalised nature of many devices, to the data and images on the device [87]. Such contextual data about the lifestyle of the user of the device, may bias the opinion of the investigator as to the guilt or innocence of an individual [103].

The requirement to allow police to view the mobile phones of rape victims, with judgements made about their appearance or lifestyle including victim blaming, can seriously prejudice investigations [118].

Example Case: Timothy Evans was tried, convicted and executed for the murder of his wife and child, but it was actually serial murderer John Christie who murdered them. Evans was prone to inventing stories about himself to boost his self-esteem. This made it difficult for him to establish credibility when dealing with the police and courts during his trial [54]. Evans was posthumously pardoned [3].

Bias 8: Software Infallibility: There is a widely-held belief that computer-generated evidence is reliable and trustworthy [64, 11, 16, 16]. This belief leads to the conclusion that any faults that manifest must have their source in the actions of the human operator [55]. If such assumptions and biases are allowed full rein, particularly when computerised technology is involved, the outcome could be an assumption of guilt. In reality, as pointed out by Mason and Seng [67] and Christie [16], faults in software are common, and defects in hardware are not impossible, especially as such hardware ages. Biases may also be inadvertently written directly into the software resulting in false positives and erroneous outputs. Finally, software systems can also be compromised by malicious external actors, such as cyber criminals, when vulnerabilities are exploited. As Partridge [77] says, IT systems will *always fail* and do not deserve the faith that ordinary citizens place in them.

Example Case: An example case is that of Nijeer Parks, detained because a facial recognition algorithm developed by Clearview AI wrongly matched him to charges of shoplifting, assault and drug possession [31]. After the error emerged, New Jersey's attorney general, Gurbir Grewal, told police to stop using facial recognition technology [27].

2.3 Addressing Human Bias

Addressing human bias in investigations begins with awareness and reflection on the known biases, whilst acknowledging the existence and influence of unconscious or unknown biases. This understanding enables investigators to recognise that there are biases in any human centred (or, for that matter, non-human) investigation, thereby providing a starting point to address them. Several mechanisms and approaches have been proposed that seek to minimise the effects and impact of human bias.

Dror [23] suggests several mechanisms investigators can adopt. Perhaps the most obvious and crucial initial step is to recognise the existence of bias from the outset of the investigation, and actively to challenge it.

(1) Investigator Training & Support: Regular unconscious bias training is essential [56, 22]. Ditrich [22] recommends that investigating officers establish a network with other investigators to exchange experiences and provide advice. Dror [23] proposes that scenarios to test multiple and competing hypotheses would help investigators to challenge their own preconceived views and biases. The importance of peer review during the investigation process is emphasised by Horsman and Sunde [47].

(2) Case Manager Role: Rossmo [92] argues that the case leader has a key role in shepherding the investigation and ensuring that investigators do not engage in tunnel vision. Dror suggests that to overcome organisational biases (e.g., time pressures, resource availability, organisational culture, etc.), case managers should control the flow of information, its timing and its relevance [23]. In addition, compartmentalisation to further address contextual bias should be adopted. Rassin recommends that investigators commence by generating multiple and competing hypotheses [88] to deliberately mitigate against a tendency to tunnel vision.

(3) Investigator Independence: Demonstrating independence is an essential obligation in internal investigations [10]. Bigler *et al.* [10] suggest that the forensic expert, investigator and author of the final report be three different and independent people. They also argue that if investigators/forensics experts/authors are employees of the company who instigates the investigation, they have to provide a statement explaining how they ensured their independence throughout the process.

(4) Data Collection & Analysis: At least two different digital forensics software tools should be used to acquire data [1, 9, 25]. Marshall *et al.* [65] argue that the organisation's information security standards and processes be examined. They should report on the relevant penetration tests that have been carried out to ensure that software vulnerabilities have been removed.

If independent investigators are involved, they should then meet to argue their different explanations for the events that triggered the investigation [47].

(5) Reporting: Marshall *et al.* [65] argue that computer bugs *must* be fully disclosed, even if corrected. The software supplier has to provide information beforehand on relevant audits that have been carried out to ensure that standards have been adhered to. Software suppliers should also be required to provide evidence of error reports and system changes and be able to demonstrate that they have implemented measures which can detect malfunctioning software.

2.4 Synopsis

This section has provided an overview of a range of human biases that can impact digital investigations, and a range of mitigation approaches that can be deployed. In order to lay the foundations for our proposed framework for ensuring that digital forensics investigations resist such biases, we now examine an eminent, recent case. This case is characterised by a number of biases whose effects could have been mitigated, had such biases been acknowledged and neutralised during investigations.

3 Analysis of the Post Office Horizon IT Case

The Post Office prosecuted and sometimes convicted their own sub-postmasters and -postmistresses of fraud and theft over the course of the previous decade [80]. (Please note that for the rest of this document we will use

the term ‘subpostmaster’ to refer to both genders). The majority of these cases relied on evidence generated by their own Horizon software system [7]. The Post Office carried out their own in-house investigations relying on software-generated evidence [16].

3.1 The HORIZON Software System

The Horizon software system cost £1 billion and was designed by ICL/Fujitsu Services [50, 33]. According to Post Office Ltd, the name ‘Horizon’ encompasses [33]: (1) the software, both bespoke and software packages, (2) the computer hardware and communications equipment installed in branch, (3) the central data centres, (4) the software used to control and monitor the systems, and (5) the testing and training systems.

The system was piloted in 1995, alongside a joint work programme between the Department of Social Security’s Benefits Agency and Post Office Counters Ltd. The aim was to provide an automated system for issuing benefits payments. ICL won the contract for further development and roll out to all Post Offices in May 1996 [73]. ICL became part of Fujitsu in 2001 [61]. Fujitsu was responsible for the maintenance of Horizon software system for the majority of the period under discussion in this paper [122].

3.2 Prosecutions

Figure 4 shows the number of prosecutions the Post Office engaged in since 1989 [83]. It is striking to notice that the number of prosecutions leaps as the Horizon system is rolled out. The second graph shows that prosecutions of sub-postmasters trend upwards, whilst prosecutions of assistants and employees have a horizontal trend. In order to provide an overview of the events and causes that characterised the Post Office Horizon IT case, we conducted a *System Theoretic Accident Model and Process* (STAMP) analysis, which we report in the next section.

3.3 System Theoretic Accident Model and Process (STAMP)

STAMP originated from the consideration that traditional event-chain models are not appropriate in describing accidents occurring to complex socio-technical systems [59, 60]. The definition of “accident” needs to be expanded beyond its traditional meaning, to encompass any “unplanned or undesired loss event” [57, p.73]. CAST (Causal Analysis based on STAMP) is utilised to understand accidents’ root causes by analysing how the broad socio-technical system contributed to the accident, beyond a specific failure event.

STAMP (and CAST) is based on three main components: (1) safety constraints (operational controls in place to avoid the occurrence of risks, hence accidents); (2) hierarchical safety control structure (systems are based on a hierarchy in which a higher level imposes a safety constraint on the lower level); (3) a two-way communication channel exists between the levels in which constraints are enforced from the higher to the lower

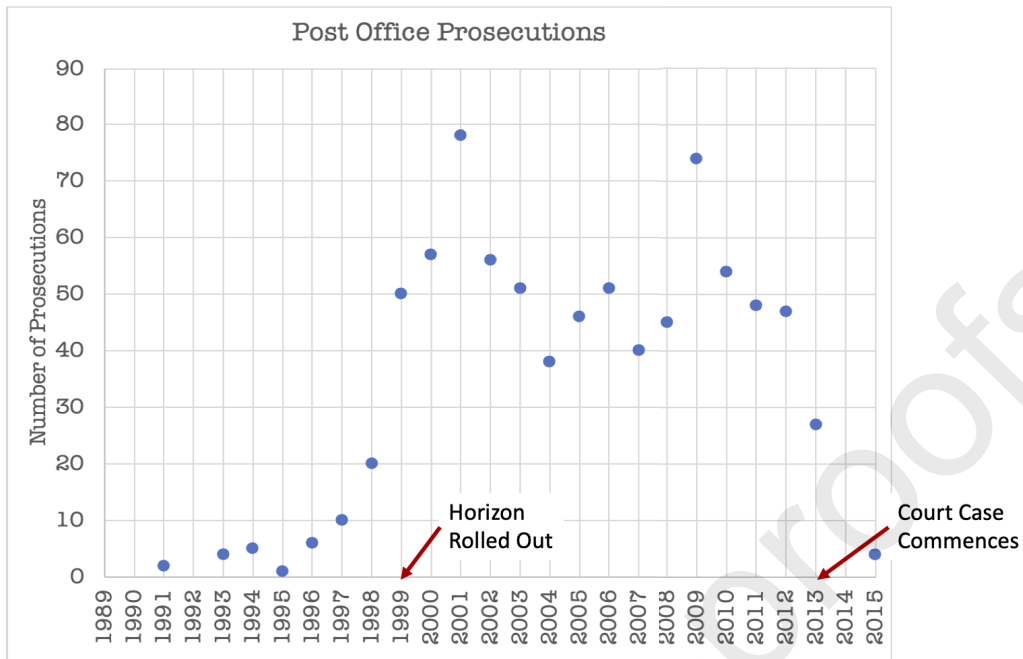


Figure 3: Post Office Prosecutions (Chart produced from information provided to FOI Request [83])

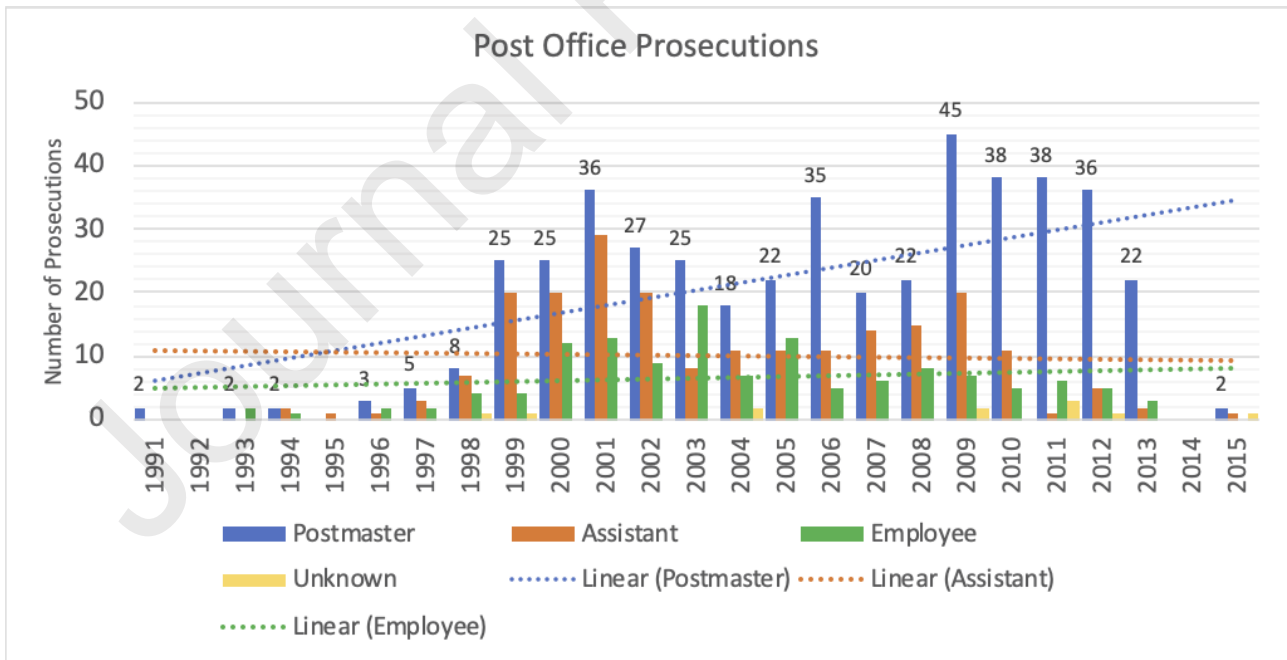


Figure 4: Post Office Prosecutions of Employees in different roles with trend line demonstrating increase in subpostmaster prosecutions. (Chart produced from information provided to FOI Request [83])

level and feedback on the effectiveness of such constraints are exchanged from the lower to the higher level); and process model (for effective control on the lower level processes, the higher level needs a model of the process being controlled). Researchers have used STAMP to analyse other software bugs and cyber-attacks [51, 106, 97], which sets a precedent for its use to study the Post Office Horizon IT case. Moreover, recent research has explicitly called for applying the framework underlying STAMP (STPA) to audit activities in computer-based evidence cases [16]. In the following points 1-9, we follow advice provided by Leveson [58, 98] in the STAMP analysis process (in its CAST formulation), to model the socio-technical system in which the case unfolded. Our analysis focuses on the Horizon software system and its poor performance, as this is the core component from which events in the case originate.

1: Identify the system and hazard associated with the accident or incident

As described in Section 3.1, we have:

The SYSTEM: The Horizon software system, an electronic accounting system deployed at UK Post Offices, developed by ICL which was subsumed by Fujitsu [122].

The HAZARD: In the timeframe of this case (in the versions of the software pre-2017) [114, 80], the Horizon software system suffered from ‘bugs’ which appeared to generate spurious duplicate or erroneous transactions, not matching the records held by the sub-postmasters [16]. Based on the erroneous transactions, the Post Office prosecuted sub-postmasters whose end-of-day Horizon software displays did not match the amount of money in the till: essentially creating shortfalls [113, #7]

2: Identify the system safety constraints and system requirements associated with that hazard

2.1 Bug-Free Software: The Horizon software system should not operate in a way that generates erroneous or duplicate transactions (requirement). The Horizon software system must have warnings and controls in place that enable detection of wrongful transactions or presence of ‘bugs’ that assure the aforementioned (requirement). The Post Office (and/or Fujitsu, based on contractual arrangements) must investigate reported anomalies with the Horizon software system (requirement). The Post Office must act upon identification of bugs in the Horizon software system (requirement). Fujitsu must eliminate bugs in and maintain the Horizon software system (requirement).

2.2 Adequate Training: The sub-postmasters should not be allowed to operate the Horizon software system without the requisite skills (constraint). The Post Office must provide adequate training to sub-postmasters on the use of the Horizon software system (requirement).

2.3 Adequate Helpline Support: The sub-postmasters should not be left without support when they detect anomalies with the Horizon software system. The Post Office must provide a help-desk staffed by well-trained staff to support sub-postmasters with respect to the Horizon software system, particularly during the first stages of its deployment (requirement). The Horizon help desk must provide effective support to sub-postmasters when the Horizon system does not perform as expected (requirement).

2.4 No Pre-Investigation Liability: The sub-postmasters should not be held accountable for errors emanating from the fallibility of the Horizon software system (constraint). The Post Office must put in place measures to protect sub-postmasters in case Horizon does not work properly (requirement).

2.5 Fair Contracts: The sub-postmasters' contracts must protect them from losses caused by bugs in the Horizon software system (requirement).

2.6 Adequate Maintenance: The Post Office must require Fujitsu to fix the bugs associated with the Horizon software system (requirement) and/or consider switching to another IT system should the Horizon software bugs not be correctable (requirement).

2.7 Union supporting Sub-postmasters: The sub-postmasters must be supported by the National Union of Sub-Postmasters (requirement).

2.8 Government Oversight: In terms of government oversight, the Post Office's 2018/19 annual report lays out the oversight arrangements [82]. The Post Office is a State-owned private company limited by shares with 4,391 employees [82]. Post Office Limited ("the Company") is wholly owned by the Secretary of State for Business, Energy and Industrial Strategy (BEIS). BEIS holds a special share in the Company, the rights of which are enshrined within the Post Office Limited Articles of Association² [82]. BEIS has the right to appoint Non-Executive Directors to the Board and typically appoints a UKGI employee for this purpose, who is required to carry out oversight of all the Post Office's activities (requirement).

2.9 'Benefit of the Doubt' Investigations: Any discrepancies between transaction records held at post offices and recorded by the Horizon software should be objectively investigated, without any initial presumption of wrongdoing by sub-postmasters (requirement).

²<http://corporate.postoffice.co.uk/our-leadership>

3: Document the safety control structure in place (development and operations)

We offer here a brief overview of the safety control structure in place in the Post Office Horizon IT case, with particular reference to governance and managerial structures.

Post Office Management & Structure

The Board of Directors of the Post Office is responsible for setting the strategic aims of the company, putting in place the leadership to deliver them, maintaining appropriate oversight of the management of the business, reporting to the shareholder and determining the company's vision, values and organisational culture [82].

The Board is accountable to the Secretary of State for BEIS, as the sole shareholder, for the performance of the company, and is required to seek consent for certain matters, as included in the Articles of Association. The shareholder is briefed regularly on the performance of the business and the progress to deliver the strategy [82].

Individual Post Offices

Post Offices are independent outlets that combine a retail shop with the Post Office branch and owned by: a multiple retailer (e.g., W. H. Smith), or a company under a franchise arrangement with the Post Office Ltd, or by an individual sub-postmaster³. The Post Office requires sub-postmasters to sign a contract with them in order to run a Post Office within the independent outlet.

Post Office Investigators

The Post Office investigators would be tasked to investigate anomalies in the first instance. A response to a FOI request [84] explains that Post Office investigators are trained to rigorous standards and operate in accordance with all requisite legislation, including the Police & Criminal Evidence Act, the Regulation of Investigatory Powers Act and the Postal Services Act. Security managers normally have experience in a wide range of operational and commercial areas. They develop technical competence in fields such as crime, risk management and modelling, electronic and mechanical security and behavioural security.

4: Ascertain the proximate events leading to the accident or incident

Figure 5 depicts the chain of events in the Post Office Horizon case. Supplementary material reported in the following sections provides evidence of each of these.

³https://www.hse.gov.uk/foi/internalops/sims/cactus/5_04_51.htm

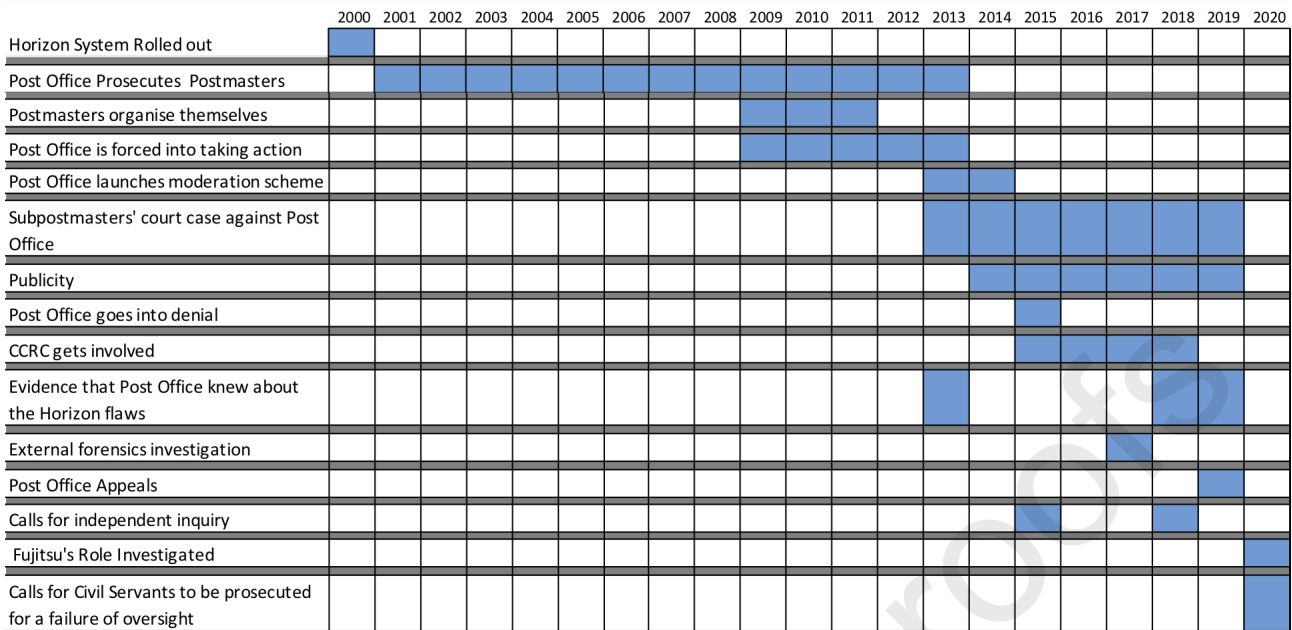


Figure 5: Chain of Events (supplementary files)

5: Analyse the accident or incident at the physical system level:

In 2012, the growing number of prosecutions led the Post Office to commission forensic accountancy firm Second Sight to carry out a forensics analysis of Horizon [36]. The investigation raised issues about how fit for purpose the Horizon IT system was, as epitomised in the following statement in Second Sight's report *"For the Horizon system to be considered fully 'fit for purpose' for all users, it would, in our opinion, need to accurately record and process, with a high degree of error repellency, the full range of products and services offered by Post Office, whilst providing a clear transactional audit trail allowing easy investigation of any problems and errors that arise. The cases that we have reviewed demonstrate that this design objective has not always been achieved"* [99, p. 42]. The report by Second Sight also stated that *"branches with unreliable hardware, or poor telecommunications and power services and supplies, appear to have suffered a disproportionate incidence of problems"* [99, p. 43]. Despite this, the Post Office maintained their position that the Horizon IT system operated correctly [69].

6: Move up the hierarchy of the safety control structure

6.1 Bug-Free Software (as per 2.1):

The Post Office refused to believe in the innocence of the sub-postmasters when they reported anomalies, even as the number of reports increased [16]. Hence, we can conclude that the safety constraints and requirements were not completely identified. There appears to have been an initial poorly-grounded assumption of correct functioning and then a determination not to change this stance when evidence increasingly emerged to suggest that the system was displaying erratic behaviours [36, 16, 80].

As reported in [14, 69, 114], Fujitsu seemed aware of issues existing with the software. Slingo [102] reports that Mr. Justice Fraser, High Court judge in the Bates vs Post Office judgement [114] expressed “*very grave concerns*” about the evidence offered by Fujitsu staff in the Crown court, in actions brought by the Post Office, and the High Court.

6.2 Adequate Training (as per 2.2):

Several sources around the Post Office Horizon IT case highlighted issues around the training that sub-postmasters received on the use of the software, its maintenance, and the reporting of any issues arising [80, 114]. If not preventing the case from unfolding, adequate training on the use of the Horizon software system could possibly have helped some sub-postmasters identify precisely where the issues were at an operational level. On this note, the Post Office themselves, in responding to the Second Sight report, admit that their training could have been improved [81].

6.3 Adequate Helpline Support (as per 2.3):

Evidence from the court case [114] cites cases where sub-postmasters detected anomalies and reported them, only for the Horizon software system Helpline to tell them that they could not find anything wrong [64]. Other sources confirm that the help desk did anything but provide assistance [80] and there is also evidence that many people abandoned their calls because they could not get through [17]. Deirdre Connolly did get through but found the help desk to be ‘useless’, saying “*They could never actually explain anything, how to do anything... I didn’t know what I was doing*” [120]. One of the witnesses during the trial said “*there were many calls to the help desk*”. The Post Office countered that problems were “*caused by human errors or other errors in transaction recovery*” [114, #216].

The question we have to ask is whether a system that leads so many of its users to make errors can be considered to be bug free [16]. A bug is not only something buried in the code of the system. A poorly designed user interface that affords multiple errors can also be considered to constitute a bug. There is evidence that the sub-postmasters considered that the system’s interface had not been designed with their needs in mind [109].

6.4 No Pre-Investigation Liability (as per 2.4):

Sub-postmasters should have been protected from erroneous operations independent of their actions. To do so, contractual arrangements should have been in place to provide details on mitigation strategies. Evidence from the case indicates that in sub-postmasters’ contracts there was no mention of the Horizon software system or associated mishaps [122, 66]. As a consequence, the correct functioning of the system can only be ascertained by Post Office senior managers’ statements which, as we saw, denied the existence of any issues.

6.5 Fair Contracts (as per 2.5):

In his ruling, Mr. Justice Fraser emphasised that some components of sub-postmasters' work contracts were unreasonable and 'onerous', and the Post Office was exercising a position of power *vis-a-vis* the sub-postmasters. The Judge ruled that the Post Office showed "oppressive behaviour" [113, #222] in response to claimants accused of accounting errors they blamed on Horizon software system. Mr. Justice Fraser stated also the following: "*The Post Office appears, at least at times, to conduct itself as though it is answerable only to itself. The statement that it is prepared to preserve documents – as though that were a concession ... and to refuse to produce them, is extremely worrying. This would be a worrying position were it to be adopted by any litigant; the Post Office is an organisation responsible for providing a public service, which in my judgement makes it even worse.*" [113, #523]

"It was expressly submitted by the Post Office – and also put to some of the Lead Claimants – that a [sub-postmaster] did not have to accept debts with which they did not agree at the end of a branch trading period. That proposition is plainly incorrect in fact." [113, #552].

6.6 Adequate Maintenance (as per 2.6):

Fujitsu should have been required to remove the bugs from the system. They appear to have attempted to do so, but some of them reappeared weeks later [114]. Service-level agreements were in place between the Post Office and Fujitsu, another control to ensure adequate performance of the managed systems, but these do not appear to have been enforced. This also demonstrates how Fujitsu was under notable budget pressures [37] and it is likely that the development team had to balance between developing new features and fixing existing issues. Finally, the Post Office considered the option of abandoning the Horizon software system [32], but decided that replacement was too risky [34].

6.7 Government Oversight (as per 2.8):

Early in 2020, there were calls for civil servants to be prosecuted for failing in their duty of oversight of the Post Office. Their inaction allegedly allowed the case to develop and prosecutions to continue unchecked from 2001 to 2009 [18]. In a House of Commons debate, Mr Jones says there was: "*little or no insight in terms of oversight from Government*" [45]. Structural limitations, apparently, also exist that have the potential to limit government's possibility of oversight in cases similar to the Post Office one. By initiating private prosecution, in fact, the Post Office was at the same time victim, prosecutor, and investigator on the case [80], as separation of responsibilities did not apply to the Post Office at the time [16], a situation that has been questioned since the case ruling [125].

6.8 ‘Benefit of the Doubt’ Investigations (as per 2.9):

The reliance on software-generated evidence and the presumption of computer dependability have raised issues around the lack of ‘benefit of the doubt’ that sub-postmasters did not enjoy in the investigations carried out by the Post Office. The behaviours of the Post Office in the private investigations on the case led Christie [16] to refer to this situation as *user error bias*, whereby “*the willingness...to absolve the system of blame and accuse users instead was such a constant theme*”.

7: Analyze overall coordination and communications as contributors to the accident or incident

In order to abide by the safety constraints and meet the requirements identified in (2), the safety control structure in place should enable an effective feedback loop, whereby the lower hierarchical level is communicated a control, and in exchange it provides information to the higher level on how the control is performing. The higher level needs to have a model of the investigation process to ascertain if the appropriate performance is achieved. We can now address each of the controls and requirements.

At the lowest hierarchical level, the sub-postmasters were operating the transactions, through the Horizon software system, at the Post Offices. To work properly, this component of the safety control structure would have needed a feedback loop between the Post Office and the sub-postmaster. In this, the Horizon software system should have acted as the communication channel between the two, provided that the information exchanged was reliable. However, as the STAMP model presented in the previous sections showed, this was not always the case. When the sub-postmasters complained to the Post Office that the Horizon software system was reporting erroneous data, the Post Office did not believe what the sub-postmasters were saying and instead trusted the Horizon software system [16]. Moreover, since the sub-postmasters were not in a position to ascertain exactly what was wrong with the Horizon software system, their claims were broadly dismissed. This component of the safety control structure relied on three communication channels: (1) from Post Office to the sub-postmasters; (2) from the Horizon software system to the Post Office; and (3) from the sub-postmasters to the Post Office. An additional level in the safety control structure involves Fujitsu, which was involved in a feedback loop of its own with the Post Office. As the number of anomalies reported by the sub-postmasters was increasing, the Post Office should have approached Fujitsu to investigate whether such claims could be accurate. Upon inspection, Fujitsu should have ascertained that the Horizon software system was not performing as expected, and then fed this back to the Post Office. The Post Office should then have acted to remediate, as a consequence. Evidence in the case demonstrates that, at some stage (likely around October 2012), Fujitsu and the Post Office did have an exchange of information regarding ‘Receipts/Payments Mismatch issue notes’ [114]. To synthesise our STAMP analysis of the case, an overview of the safety control structure, feedback loops, and notations related

to their failures, is provided in Figure 6.

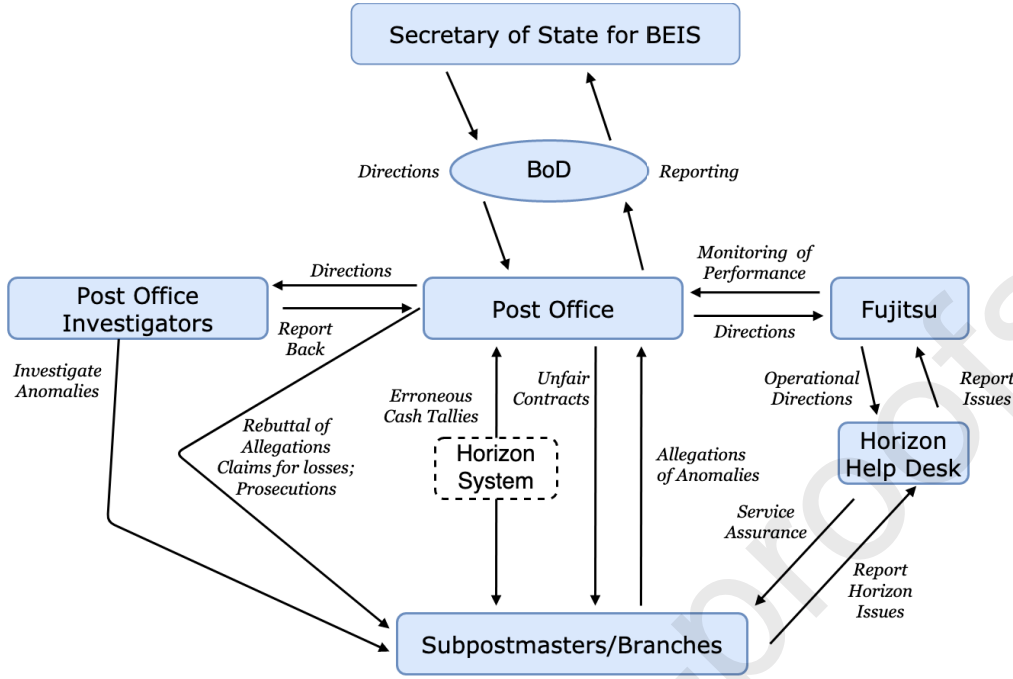


Figure 6: STAMP Analysis of the Post Office Horizon-Related Events

8: Determine the dynamics and changes in the system

In order to offer an understanding of some of the deepest factors influencing the development of the Post Office Horizon IT case, we now briefly summarise some of the root causes that may have contributed:

RC1: Software Bugs & Denial Thereof: (potentially relevant biases: Bias 1: Confirmation Bias; Bias 8: Software Infallibility; Bias 5: Irrelevant Information; Bias 6: Reference Material)

It is evident that between 2000 and 2019 there was a presumption that evidence produced by computers was considered to be absolutely reliable in court. The accused needed to prove the contrary [64, 16],[113, #145]. Moreover, at the trial level, sub-postmasters were not given the information they needed to counter what the Horizon software system was displaying, raising questions about the degree of disclosure by the Post Office [64].

The Horizon software had some bugs, that could cause intermittent errors [99]. Second Sight carried out an extensive review of the system, reporting that whilst the system normally behaved correctly, “*occasionally errors occur or disputes arise*” (p.5) [99].

The aforementioned review identified a number of potential causes for anomalies generated by Horizon: (1) old and outdated hardware and technology, (2) issues with telecommunications equipment, (3) inadequate usability testing, (4) an icon-based user interface, (5) software that allowed multiple logins by the same user, (6) lack of secure authentication, (7) lack of anomaly detection functionality within the software and (8) a failure

to implement approval processes within the software. Further, recent research has highlighted the practice, emerged from the judgement [114], of the Post Office granting powerful user privileges to some of its users, and using this as a method to create, amend or delete production data [16], a practice which should normally be used only in exceptional circumstances.

Mr Justice Fraser, who oversaw the multiparty litigation case of 2019, found the associated prosecutions, based on software generated evidence, to be unsound. He said *“In my judgement these submissions by the Post Office are bold, pay no attention to the actual evidence, and seem to have their origin in a parallel world.”* [114, #138].

RC2: Contract Issues: (potentially relevant bias: Bias 2: Training & Motivation)

The Post Office Horizon IT case was characterised by organisational issues that, Mr. Justice Fraser noted, materialised in lack of equity in how work contracts were drafted between the organisation and the sub-postmasters. If someone wished to become a sub-postmaster, then it was the Post Office’s terms that were available, and those terms alone. This is demonstrated, for example, in the following statement (where SPM stands for sub-postmaster): *“There was no negotiation permitted whatsoever. The Post Office is also a sizeable and significant institution. A SPM is a small business person, although some may have more than one branch. The two parties are not remotely equal. In fact, they are almost uniquely unequal.”* [113, #1098].

The Post Office investigators told several sub-postmasters experiencing issues with Horizon IT that they were the only ones affected by such issues [91], nor did they tell at least one sub-postmaster that their own employee had pointed to a Horizon system issue possibly being the source of shortfalls [113, #146]. The Post Office’s response to anomalies, and contested balances, was to generally demand that sub-postmasters make up the deficiencies [113, p.18].

RC3: Institution Culture: (potentially relevant biases: Bias 4: Base Rate Expectations)

Hassall and Tucker [46] mention in a BBC report the case of an ex-employee stating that “there was no space for honesty, no desire for open dialogue.” Also that: *“It felt as though doing the right thing no longer mattered, it was all about saving the image of the Post Office”*.

The Judge hearing the case ruled that Post Office showed “oppressive behaviour” in response to claimants accused of accounting errors they blamed on Horizon software system [38]. Also, Mr. Justice Fraser reports that: *“The Post Office appears, at least at times, to conduct itself as though it is answerable only to itself. The statement that it is prepared to preserve documents – as though that were a concession – and... to refuse to produce them, is extremely worrying. This would be a worrying position were it to be adopted by any litigant; the Post Office is an organisation responsible for providing a public service, which in my judgement makes it even worse.”* [113, #523] and also *“It was expressly submitted by the Post Office – and also put to some of the*

Lead Claimants – that a Sub-postmaster did not have to accept debts with which they did not agree at the end of a branch trading period. That proposition is plainly incorrect in fact.” [113, #552].

RC4: Privatisation of the Post Office & Lack of Government Oversight: (potentially relevant biases: Bias 4: Base Rate Expectations; Bias 6: Reference Material)

Recent trends and organisational change through which the Post Office has passed, could have had an impact in this case. In several pieces of evidence, it has been demonstrated that the growing number of activities (some of them of a more corporate type, than a public service one) taking place in Post Office branches, may have rendered the environment particularly complex [42, 94]. The Horizon software system itself has been described by several sources as specifically complex [114]. With increasing complexity often also comes increasing system vulnerability to disruptions [62], a concept brilliantly captured by Charles Perrow in his definition of *interactive complexity* [79].

RC5: Internal Investigations & Prosecutions: (potentially relevant bias: Bias 4: Base Rate Expectations)

The Post Office investigated the alleged fraud themselves and then prosecuted their sub-postmasters (The Post Office is considered the world’s oldest prosecuting authority [115], with this right dating back to 1683 [93]). This demonstrated a problematic lack of separation of responsibility [113]. Forty seven were convicted of a range of fraudulent activities, with some being incarcerated as a consequence [101]. Others avoided convictions by borrowing money to make up shortfalls [80].

During parliament questions, Ian Henderson, one of the investigators from Second Sight, said that “*The approach of the Post Office’s in-house investigations team was said to be flawed: ‘problems with Horizon were effectively off limits to investigators, who, as a matter of policy, were not allowed to consider Horizon as the cause of the reported shortfalls’*” [125]. During the same session, it was explained that the Post Office’s own internal investigators carried out investigations, and used their in-house lawyers to prosecute its own workers.

9: Generate recommendations

In line with the STAMP analysis, the next step would usually focus on producing recommendations to improve the *status quo*. To do so, we decided to focus on the investigation component of the Post Office Horizon IT case and draw recommendations that are applicable to other cases in which important evidence is computer-generated. Our recommendation is that a framework be formulated, which guides investigators through the investigation process highlighting potential bias in such instances. We propose a framework that maps biases to mitigation measures, as depicted in Figure 7. Its use could be mandated by the courts in cases where investigations of potential fraud take place, particularly where evidence is generated by a software system. In

the next Section, we examine the details of this proposed framework, and report on our evaluation thereof.

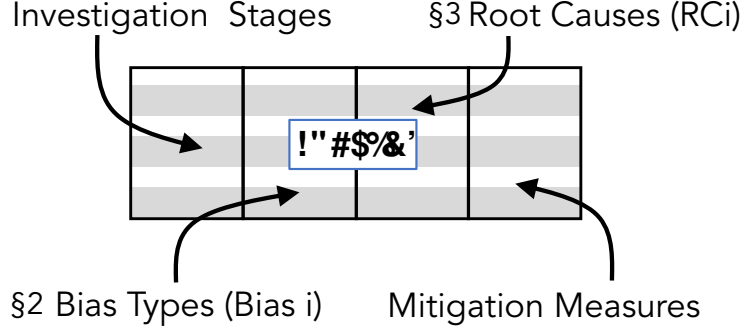


Figure 7: A framework to neutralise investigator bias

4 A Framework to Prevent Miscarriages of Justice

First, we justify our choice of a foundational framework to extend for our purposes (Section 4.1). Then, we explain how we extended the FORZA framework [49] to mitigate the different kinds of biases that can emerge in investigations characterised by large-scale use, of computer-based evidence.

4.1 Identifying a Foundational Framework

There are many digital forensics frameworks e.g., [29, 52, 8]. All have merit but we needed one that could easily be extended to address the human biases that can lead to root causes and events such as the ones emerging in the case we analysed. Jeong [49] proposes a FORZA framework, which suggests a cross-section of 8 layers and 6 questions. This crucially includes the legal requirements of such investigations. This question-based structure also lends itself very well to extensions such as the one we propose. To develop PRECEPT-4-Justice, we added another dimension: **Mitigation** i.e., which human bias(es), as enumerated in the previous section, could possibly introduce subjectivity into investigations — and a suggestion for mitigation thereof (Figure 8).

4.2 Evaluation of PRECEPT-4-Justice Framework

The key part in evaluating the framework is to measure the impact of the framework extension i.e., how effective it will be to take the various biases into consideration during an investigation. In order to carry out the evaluation, a set of questions were utilised, and put to selected practitioners and professional respondents. The questions are provided in Appendix A. Evaluators were provided with Table 2, which offers details of the mappings from the FORZA investigation stages to the biases and the root causes we identified during our analysis of the Post Office case, and then to investigation-specific mitigations identified from the research








	WHY	WHAT	HOW	WHERE	WHO	WHEN	MITIGATE
Investigation							
Contextual							
Advisory							
Conceptual Security							
Technical Preparation							
Data Acquisition							
Data Analysis							
Legal Presentation							
							

Figure 8: First draft PRECEPT-4-Justice investigation framework (extending Jeong’s FORZA framework [49])

literature. The feedback from the respondents was reviewed to refine and improve the final PRECEPT-4-Justice framework.

The evaluation sets a baseline, that is to say, the situation for the case study before the PRECEPT-4-Justice framework is applied. The baseline will take into account the legal and procedural aspects of digital investigations encoded in the FORZA framework [49], which PRECEPT-4-Justice extends with an extra dimension: *mitigation* of human bias. The recommendations that can be applied to neutralise and prevent such biases from influencing the objectivity of an investigation are informed by the research literature covered in Section 2, as well as the digital forensics literature addressing the impact of human bias on forensic investigations.

The final part of the evaluation will be based on the explanation, using the PRECEPT-4-Justice framework, as a justification for potential positive differences in the outcome from the Post Office case study, if this extended Framework had been used.

Evaluation: Expert Participants

The PRECEPT-4-Justice framework was evaluated by digital forensics practitioners. Evaluators were recruited using convenience sampling, via a request sent out to digital forensics investigators the authors knew. In total, 10 evaluators (6 academics, 3 practitioners, and 1 who is both) gave their opinion as to the power of the framework to make a difference to forensics investigations.

9 of 10 evaluators considered the framework to be self explanatory. The tenth would have liked to see more information about software testing, in terms of how this ought to be carried out with rigour. Their direct quotes are provided in Appendix B. In summary, the feedback highlighted the following issues:

1. Generating multiple hypotheses at the outset could engender bias.
2. A number raised concerns about resourcing implications. We had suggested that multiple investigators carry out independent investigations, and this is admittedly more resource intensive than usual investiga-

tions. The evaluators pointed out that, for many organisations, this would be infeasible.

They question our suggestion related to using two tools, which also might not be feasible, given the amount of time it would take to do this. They are not convinced that one piece of forensics software would extract different evidence from another. E10 also pointed out that if two tools are used, the investigator should ensure that they use different libraries.

3. A number of evaluators expressed reservations about any framework offsetting the tremendous pressures and biases that shape investigations. They ask why we did not recommend that external investigators carry out investigations. The Post Office Horizon IT case highlights how there is some merit to this suggestion: Second Sight (the external forensics accountant company involved in the case) cast light on some of the issues that emerged with Horizon IT. Yet external investigators are also human, and thus also subject to unconscious bias.

5 Final PRECEPT-4-Justice Framework

The following changes were made to the framework in response to the evaluation process. The final framework is presented in Table 1:

1. We retained the initial formulation of multiple hypotheses, given that the evaluator’s comment referred to criminal investigations, which are different from digital forensics investigations. It was felt by all the other evaluators that the use of multiple hypotheses right at the outset would deliver value in terms of making the investigator aware of the possibility of other explanations for anomalies, and requiring them to investigate each of these.
2. We have split the framework recommendations into ‘essential’ and ‘if feasible’ actions, with the latter being constrained by resource implications, as recommended by a number of the evaluators.
3. We have removed the need for the investigator to verify the correctness of the software as part of the investigation, as recommended by E9. We have recommended that evidence of actions verifying the software be provided to the investigator.
4. While external investigations might be best, many organisations do indeed prefer to carry out internal investigations, and in these cases it might not be possible to outsource this. In these cases, PRECEPT-4-Justice could provide assistance.

Table 1 outlines the final, refined framework. Given the feedback provided by our expert reviewers, we acknowledge that our framework attempts to achieve the status of “gold standard” for ensuring non-biased

investigations. However, reality suggests that it could not be feasible/viable in all cases. In particular, where resourcing is a concern, investigators could deploy only *essential* mitigations.

5.1 Application of PRECEPT-4-Justice to mitigate issues that emerged in the Post Office case

RC1: Software Bugs and Denial Thereof & RC2: Contract Issues: During the first level, the establishment of competing hypotheses serves to ensure that tunnel vision does not establish itself from the outset, and that guilt is not automatically assumed [35]. Examination of error logs, maintenance reports and information security processes during advisory and conceptual security levels can help investigators verify the correctness of the software, instead of assuming that it is functioning correctly [36]. Moreover, in not assuming guilt, sub-postmasters would not be required to make up shortfalls without objective investigations.

RC3: Institution Culture & RC5: Internal Investigations & Prosecutions: Appointing a case manager and ensuring that they are well informed of all the facts of the case should help ensure a measure of shepherding through the investigation process. Assuring investigator independence allows them to unravel the actual causes of anomalies and discrepancies, instead of being pressured to find for the institution [121].

RC4: Privatisation of the Post Office & Lack of Government Oversight: cannot be addressed by an investigation framework, since it refers to a lack of oversight over the Post Office’s handling of the affair [48]. Any oversight committee could, however, mandate the use of PRECEPT-4-Justice in investigations to prevent issues similar to RC4.

5.2 Limitations & Future Work

While we did ask forensics evaluators to provide feedback on our framework, we acknowledged that the framework itself has not been evaluated in an actual investigation, nor have any evaluation criteria been identified to do so. As such, we have some suggestions for future work:

1. Derive a set of evaluation criteria to be used to evaluate the power of PRECEPT-4-Justice in a real investigation, in terms of neutralising bias.
2. Consider development of PRECEPT-4-Technology, which tackles the issue of the trustworthiness of the technology used by investigators at each stage of the investigation. This would ensure that the investigation is not compromised by investigators trusting the outcome of forensics software without verifying it.

Table 1: Final PRECEPT-4-Justice FORZA extension

Level	PRECEPT-4-Justice Mitigation Measure	Bias
Conceptual investigation:	Hypothesis Generation: <i>Essential:</i> Generate multiple and competing hypotheses. <i>If Feasible:</i> Assign different hypotheses to different investigators.	Bias 5 & 6
Contextual Layer:	Appoint and Inform Case Manager: <i>Essential:</i> Ensure that the case manager is aware of all the information related to the case. <i>If Feasible:</i> Have an external case manager.	Bias 1
Legal Advisory Layer:	Guarantee Independence of Investigators: <i>Essential:</i> Ensure that digital investigators are independent and have no conflicts of interests. If investigators/forensics experts/authors are employees of the company who instigates the investigation, they have to provide a statement explaining how they ensured their independence throughout the process.	Bias 3 & 6
Conceptual Security Layer:	Software Security Assurances: <i>Essential:</i> Require software supplier to report their information security processes.	Bias 8
Technical Preparation Layer:	Validate Software Error Detection and Correction: <i>Essential:</i> Examine software supplier's error and maintenance log.	Bias 6
Data Acquisition Layer:	Acquire evidence using two different tools: <i>Essential:</i> Ensure that all digital evidence has been gathered and is considered as part of the investigation. Acquisition should take place according to the appropriate legal guidelines. The imaged data should be made available to 3rd party (defence). <i>If Feasible:</i> Use at least two different digital forensics software tools to acquire data. Ensure that these tools use different libraries.	Bias 4
Data Analysis Layer:	Construct timeline for each hypothesis: <i>Essential:</i> Refer back to the investigation layer, and extract information that could potentially be critical for proving each of the multiple hypotheses. Attempt to reconstruct a timeline for each of the hypotheses. <i>Essential:</i> Investigators should deliberately play devil's advocate and continuously strive for objectivity.	Bias 2 & 6
Legal Presentation Layer:	Compose reports for each competing hypothesis: <i>Essential:</i> Reports should be written. All processes used, and all results identified in data analysis should be provided in full disclosure. Ensure that the case is made for and against competing hypotheses is presented, and backed up with corroborated evidence i.e. not only software generated evidence. <i>If Feasible:</i> Independent investigators should meet to argue their different explanations for the events that triggered the investigation.	Bias 4
Across all Layers:	<i>Essential:</i> Maintain an audit trail of all decisions. <i>Essential:</i> Maintain contact with other forensics investigators if there is only one investigator on a particular investigation, to benefit from peer review and the experiences of others. <i>Essential:</i> Investigators should go on regular training so that they stay aware of the dangers of being influenced by bias during investigations.	All

6 Conclusion

The Post Office case highlights the limits intrinsic to an excessive reliance on the reliability of computer-based evidence in forensics investigations, alongside the impact of bias on those investigations. In our study, we have summarised the main components and events of the Post Office Horizon IT case by applying the STAMP model, and highlighting biases and root causes that contributed to the unfolding of events. As we finalise this paper, appeal judges have overturned the convictions of 39 subpostmasters [19]. Our work has a constructive purpose: we utilised the case to exemplify an extension of Jeong’s FORZA framework. The resulting PRECEPT-4-Justice framework has been reviewed by forensics and investigative experts, and their feedback incorporated in the final version of our framework. It is during investigations that PRECEPT-4-Justice can maximise the objectivity and consequent veracity of evidence presented to courts. Our aim is to help investigators to avoid contributing to miscarriages of justice in the future.

References

- [1] R. Adams. *The advanced data acquisition model (ADAM): a process model for digital forensic practice*. PhD thesis, Murdoch University, 2012.
- [2] K. Ask and L. Alison. Investigators’ decision making. *Forensic Psychology in Context: Nordic and International Perspectives*, pages 35–55, 2010.
- [3] R. Baker. ‘Christie Done It’ – The Last Words, Trial And Official Murder of Timothy Evans in 1950, 2014. Retrieved 24 April 2021 from: <https://flashbak.com/christie-done-it-the-last-words-trial-and-official-murder-of-timothy-evans-in-1950-17935/>.
- [4] BBC. George not guilty of Dando murder , 2008. Retrieved 24 April 2021 from: <http://news.bbc.co.uk/1/hi/uk/7536815.stm>.
- [5] BBC. G20 death: PC Simon Harwood sacked for gross misconduct, 2012. Retrieved 23 April 2021 from: <https://www.bbc.co.uk/news/uk-19620627>.
- [6] BBC. Timeline: Ian Tomlinson’s death, 2013. Retrieved 31 Jan 2021 from: <https://www.bbc.com/news/uk-10728685>.
- [7] BBC. Postmasters were prosecuted using unreliable evidence, 2020. Retrieved 15 Feb 2021 from: <https://www.bbc.co.uk/news/uk-52905378>.
- [8] N. L. Beebe and J. G. Clark. A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, 2(2):147–167, 2005.
- [9] W. A. Bhat, A. AlZahrani, and M. A. Wani. Can computer forensic tools be trusted in digital investigations? *Science & Justice*, 2020. <https://doi.org/10.1016/j.scijus.2020.10.002>.
- [10] E. D. Bigler, R. R. Green, T. J. Farrer, J. C. Roper, and J. B. Millward. The Rigor of Research Design and “Forensic” Publications in Neuropsychological Research. *Psychological Injury and Law*, 2(1):43–52, 2009.
- [11] I. Bogost. The Cathedral of Computation, 2015. Retrieved 30 Jan 2021 from: <https://www.theatlantic.com/technology/archive/2015/01/the-cathedral-of-computation/384300/>.
- [12] E. M. Borchard. *Convicting the Innocent*. Yale University Press, New Haven, 1932.
- [13] E. G. Boring. A new ambiguous figure. *The American Journal of Psychology*, 2:444–445, 1930.

- [14] R. Brooks and N. Wallis. Justice Lost In The Post, 2020. Private Eye Special Report. Retrieved 25 May 2020 from: <https://www.private-eye.co.uk/special-reports/justice-lost-in-the-post>.
- [15] casetext. People v. Tait, 1932. Retrieved 29 Jan 2021 from: <https://casetext.com/case/people-v-tait-2>.
- [16] J. Christie. The Post Office Horizon IT Scandal and the Presumption of the Dependability of Computer Evidence. *Digital Evidence & Elec. Signature L. Rev.*, 17:49–70, 2020.
- [17] T. Collins. Lives ruined by IT glitches? Post Office officials face the critics, 2015. Retrieved 2 Feb 2021 from: <https://ukcampaign4change.com/2015/02/05/lives-ruined-by-it-glitches-post-office-officials-face-the-critics/>.
- [18] T. Collins. The civil service may face an investigation into maladministration over Post Office IT scandal, 2020. Retrieved 2 Feb 2021 from: <https://ukcampaign4change.com/2020/06/03/the-civil-service-may-face-an-investigation-into-maladministration-over-post-office-it-scandal/>.
- [19] T. Collins. Post Office’s failures “so egregious as to make the prosecution of any of the Horizon cases an affront to the conscience of the court” say appeal judges today. But why no government inquiry?, 2021. 23 April <https://ukcampaign4change.com/2021/04/23/post-offices-failures-so-egregious-as-to-make-the-prosecution-of-any-of-the-horizon-cases-an-affront-to-the-conscience-of-the-court-say-appeal-judges-today-but-why-no-government-inquiry/>.
- [20] G. S. Cooper and V. Meterko. Cognitive bias research in forensic science: a systematic review. *Forensic Science International*, 297:35–46, 2019.
- [21] L. Dignan. Buggy software: Why do we put up with it?, 2010. Retrieved 16 Jan 2021 from: <https://www.zdnet.com/article/buggy-software-why-do-we-put-up-with-it/>.
- [22] H. Ditrich. Cognitive fallacies and criminal investigations. *Science & Justice*, 55(2):155–159, 2015.
- [23] I. E. Dror. Practical solutions to cognitive and human factor challenges in forensic science. *Forensic Science Policy & Management: An International Journal*, 4(3-4):105–113, 2013.
- [24] I. E. Dror. Biases in forensic experts. *Science*, 360(6386):243, 2018.
- [25] H. Earwaker, S. Nakhaeizadeh, N. M. Smit, and R. M. Morgan. A cultural change to enable improved decision-making in forensic science: A six phased approach. *Science & Justice*, 60(1):9–19, 2020.
- [26] A. Eerland and E. Rassin. Let’s find the evidence: An analogue study of confirmation bias in criminal investigations. *Journal of Investigative Psychology and Offender Profiling*, 7:231–246, 2010.
- [27] EURPublisher01. NJ Black Man Spent 10 Days in Jail After Being Misidentified by Police Using Facial Recognition Software, 2020. Retrieved 30 Jan 2021 from: <https://eurweb.com/2020/12/29/nj-black-man-spent-10-days-in-jail-after-being-misidentified-by-police-using-facial-recognition-software-video/>.
- [28] FBI. A Review of the FBI’s Progress in Responding to the Recommendations in the Office of the Inspector General Report on the Fingerprint Misidentification in the Brandon Mayfield Case, 2011. Retrieved 29 Jan 2021 from: <https://www.oversight.gov/sites/default/files/oig-reports/s1105.pdf>.
- [29] I. Ferguson, K. Renaud, S. Wilford, and A. Irons. PRECEPT: a framework for ethical digital forensics investigations. *Journal of Intellectual Capital*, 21(2):257–290, 2020.
- [30] S. E. Fiarman. Unconscious bias: When good intentions aren’t enough. *Educational Leadership*, 74(3):10–15, 2016.
- [31] A. Fitch. Facial-Recognition Tools in Spotlight in New Jersey False-Arrest Case, 2020. Retrieved 30 Jan 2021 from: <https://www.wsj.com/articles/facial-recognition-tools-in-spotlight-in-new-jersey-false-arrest-case-11609269719>.

- [32] K. Flinders. Post Office wants to get to bottom of IT system allegations, 2013. Retrieved 2 Feb 2021 from: <https://www.computerweekly.com/news/2240176122/Post-Office-wants-to-get-to-bottom-of-IT-system-allegations>.
- [33] K. Flinders. Post Office ends working group for IT system investigation day before potentially damaging report, 2015. Retrieved 2 Feb 2021 from: <https://www.computerweekly.com/news/2240242064/Post-Office-ends-IT-system-investigation-day-before-potentially-damning-report>.
- [34] K. Flinders. ‘Considerable risk’ if Post Office replaced Horizon system, says chairman, 2016. Retrieved 2 Feb 2021 from: <https://www.computerweekly.com/news/450297820/Considerable-risk-if-Post-Office-replaced-Horizon-system-says-chairman>.
- [35] K. Flinders. MET Police assessing evidence of potential perjury in Post Office IT trials, 2017. Retrieved 16 Feb 2021 from: <https://www.computerweekly.com/news/252482260/Met-Police-assess-evidence-of-potential-perjury-in-Post-Office-IT-trials>.
- [36] K. Flinders. Forensic investigation into Post Office IT system at centre of legal case nears completion, 2018. Retrieved 16 Feb 2021 from: <https://www.computerweekly.com/news/450430183/Post-Office-court-case-judge-issues-warning-to-legal-teams>.
- [37] K. Flinders. Fujitsu must face scrutiny following Post Office Horizon trial judgment, 2019. Retrieved 16 Feb 2021 from: <https://www.computerweekly.com/news/252476403/Fujitsu-must-face-scrutiny-following-Post-Office-Horizon-trial-judgment>.
- [38] K. Flinders. Subpostmasters achieve ‘stunning victory’ against Post Office in Horizon case, 2019. Retrieved 16 Feb 2021 from: <https://www.computerweekly.com/news/252459564/Subpostmasters-achieve-stunning-victory-against-Post-Office-in-Horizon-case>.
- [39] Forensic Science Regulator. Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System, 2017. Issue 4. Retrieved 19 January 2021 from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/651966/100_-_2017_10_09_-_The_Codes_of_Practice_and_Conduct_-_Issue_4_final_web_web_pdf__2_.pdf.
- [40] FPT Heads Of Prosecutions Committee Working Group . Report on the Prevention of Miscarriages Of Justice. Retrieved 29 January from: <https://www.justice.gc.ca/eng/rp-pr/cj-jp/ccr-rc/pmjp-pej/index.html>.
- [41] P. A. Fraser-Mackenzie, R. Bucht, and I. E. Dror. Forensic judgement and decision-making. In T. R. Zentall and P. H. Crowley, editors, *Comparative Decision Making*. Oxford Scholarship Online, Oxford, 2013.
- [42] N. Fuller-Love and J. Cooper. Deliberate versus emergent strategies: a case study of information technology in the Post Office. *International Journal of Information Management*, 20(3):209–223, 2000.
- [43] B. Garrett. *Convicting the innocent*. Harvard University Press, London, UK, 2011.
- [44] J. B. Gould, J. Carrano, R. A. Leo, and J. K. Young. Predicting erroneous convictions: A social science approach to miscarriages of justice. *Univ. of San Francisco Law Research Paper*, 2013-20, 2013.
- [45] Hansard. Horizon Settlement: Future Governance of Post Office Ltd, 2020. Parliamentary Debate, 19 March. Retrieved 16 Feb 2021 from: <https://www.parliament.co.uk/mp/david-jones/debate/commons/2020-03-19/debates/03E48E18-4B5E-4A42-84C3-684E6B58495D/HorizonSettlementFutureGovernanceOfPostOfficeLtd>.
- [46] H. Hassall and M. Tucker. Post Office false theft claim left me bankrupt. Retrieved 30 October 2020 from: <https://www.bbc.com/news/business-51446463>.
- [47] G. Horsman and N. Sunde. Part 1: The need for peer review in digital forensics. *Forensic Science International: Digital Investigation*, 35:301062, 2020.
- [48] House of Commons. Horizon Settlement: Future Governance of Post Office Ltd, 2020. Volume 673.

- [49] R. S. Jeong. FORZA - Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, 3:29–36, 2006.
- [50] C. Jee. Post Office obstructing Horizon probe, investigator claims, 2015. Computerworld UK Retrieved 29 March 2015 from: <http://www.computerworlduk.com/news/public-sector/3596589/post-office-obstructing-horizon-probe-investigator-claims/>.
- [51] C. W. Johnson and C. M. Holloway. The ESA/NASA SOHO mission interruption: Using the STAMP accident analysis technique for a software related ‘mishap’. *Software: Practice and Experience*, 33(12):1177–1198, 2003.
- [52] N. M. Karie and H. S. Venter. Towards a framework for enhancing potential digital evidence presentation. In *2013 Information Security for South Africa*, pages 1–8. IEEE, 2013.
- [53] S. M. Kassir, I. E. Dror, and J. Kukucka. The forensic confirmation bias: Problems, perspectives, and proposed solutions. *Journal of Applied Research in Memory and Cognition*, 2(1):42–52, 2013.
- [54] L. Kennedy. *Ten Rillington Place*. Victor Gollancz Ltd., London, England, 1996.
- [55] P. B. Ladkin, B. Littlewood, H. Thimbleby, and M. Thomas. The Law Commission presumption concerning the dependability of computer evidence. *Digital Evidence and Electronic Signature Law Review*, 17:1–14, 2020.
- [56] A. Lattal. The Hidden World of Unconscious Bias and Its Impact on the Neutral Workplace Investigator. *Journal of Law & Policy*, 24:411–466, 2015.
- [57] N. G. Leveson. *A Systems-Theoretic View of Causality*. MIT Press, 2012.
- [58] N. G. Leveson. *Analyzing Accidents and Incidents (CAST)*. MIT Press, 2012.
- [59] N. G. Leveson. *Questioning the Foundations of Traditional Safety Engineering*. MIT Press, 2012.
- [60] N. G. Leveson. *Engineering a safer world: Systems thinking applied to safety*. The MIT Press, 2016.
- [61] J. Leyden. ICL brand put to the sword, 2001. Retrieved 14 Dec 2020 from: https://www.theregister.com/2001/06/21/icl_brand_put/.
- [62] S. Lukasik. Vulnerabilities and failures of complex systems. *International Journal of Engineering Education*, 19(1):206–212, 2003.
- [63] B. A. MacFarlane and S. M. Cordner. *Wrongful convictions: the effect of tunnel vision and predisposing circumstances in the criminal justice system*. Government of Ontario Toronto, 2008.
- [64] P. Marshall. The harm that judges do – misunderstanding computer evidence: Mr Castleton’s story. *SAS Open Journals System*, 17:25–48, 2020. <https://doi.org/10.14296/deeslr.v17i0.5172>.
- [65] P. Marshall, J. Christie, B. Ladkin, B. Littlewood, S. Mason, M. Newby, J. Rogers, H. Thimbleby, and M. Thomas. Recommendations for the probity of computer evidence. *Digital Evidence and Electronic Signature Law Review*, 18:18–26, 2020.
- [66] S. Mason. Case Transcript: England & Wales - Regina v Seema Misra, T20090070. *Digital Evidence and Electronic Signature Law Review*, 12, 2015.
- [67] S. Mason and D. Seng. *Electronic evidence*. University of London Press, 4 edition, 2017.
- [68] E. Mattijssen, W. Kerkhoff, C. Berger, I. E. Dror, and R. Stoel. Implementing context information management in forensic casework: Minimizing contextual bias in firearms examination. *Science & Justice*, 56(2):113–122, 2016.
- [69] T. McCormack. The Post Office Horizon System and Seema Misra. *Digital Evidence & Elec. Signature L. Rev.*, 13:133, 2016.
- [70] S. Nakhaeizadeh, R. Morgan, and I. Dror. The Emergence of Cognitive Bias in Forensic Science and Criminal Investigations. *British Journal of American Legal Studies*, 4(2):528–554, 2015.

- [71] J. O. Newman. Beyond reasonable doubt. *New York University Law Review*, 68:979–1002, 1993.
- [72] R. S. Nickerson. Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*, 2(2):175–220, 1998.
- [73] L. Nicolle. More than the cost of a first class stamp, 2000. Retrieved 14 Dec 2020: <https://www.computerweekly.com/feature/More-than-the-cost-of-a-first-class-stamp>.
- [74] H. Oberai and I. M. Anand. Unconscious bias: thinking without thinking. *Human Resource Management International Digest*, 26(6):14–17, 2018.
- [75] C. Page. Home Office: ‘Software Bug’ Wiped 150,000 Arrest Records From Police Database, 2021. Retrieved 16 Jan 2021 from: <https://www.forbes.com/sites/carlypage/2021/01/15/home-office-software-bug-wiped-150000-arrest-records-from-police-database/?sh=13e6a8324199>.
- [76] H. Page, G. Horsman, A. Sarna, and J. Foster. A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn? *Science & Justice*, 59(1):83–92, 2019.
- [77] D. Partridge. *The seductive computer: why IT systems always fail*. Springer Science & Business Media, 2010.
- [78] J. Patzakis. Another Criminal Conviction Overturned Due to Failure to Authenticate Social Media Evidence, 2020. Retrieved 1 January 2021 from: <https://blog.x1discovery.com/2020/07/21/another-criminal-conviction-overturned-due-to-failure-to-authenticate-social-media-evidence/>.
- [79] C. Perrow. *Normal accidents: Living with high risk technologies-Updated edition*. Princeton university press, 2011.
- [80] M. Pooler and J. Croft. Bankruptcy, jail, ruined lives: inside the Post Office scandal, 2020. Retrieved 14 Feb 2021 from: <https://www.ft.com/content/0138cd7d-9673-436b-86a1-33704b29eb60>.
- [81] Post & Parcel. The UK’s Post Office responds to Horizon report, 2015. Retrieved 15 Feb 2021 from: <https://postandparcel.info/64576/news/the-uks-post-office-responds-to-horizon-report/>.
- [82] Post Office. Post Office Limited Annual Report & Consolidated Financial Statements 2018/19, 2019. Retrieved 16 Feb 2021 from: http://corporate.postoffice.co.uk/media/46797/2019_annualreport_final_signed.pdf.
- [83] Post Office. Freedom of Information request to Post Office Limited by Nick Wallis: Prosecutions and convictions since 1990, 2020. 9 April. Retrieved 16 Feb 2021 from: https://www.whatdotheyknow.com/request/prosecutions_and_convictions_sin.
- [84] Post Office. Freedom of Information request to Post Office Limited by Peter C. Bell: Current guidance to Post Office prosecutors and/or investigators, 2020. 9 April. Retrieved 16 Feb 2021 from: https://www.whatdotheyknow.com/request/current_guidance_to_post_office#incoming-1636782.
- [85] S. Poyser and R. Milne. No grounds for complacency and plenty for continued vigilance: Miscarriages of justice as drivers for research on reforming the investigative interviewing process. *The Police Journal*, 88(4):265–280, 2015.
- [86] E. Pronin, D. Y. Lin, and L. Ross. The bias blind spot: Perceptions of bias in self versus others. *Personality and Social Psychology Bulletin*, 28(3):369–381, 2002.
- [87] A. Quigley-McBride. Practical solutions to forensic contextual bias. *Zeitschrift für Psychologie*, 228:162–174, 2020.
- [88] E. Rassin. Reducing tunnel vision with a pen-and-paper tool for the weighting of criminal evidence. *Journal of Investigative Psychology and Offender Profiling*, 15(2):227–233, 2018.
- [89] J. Robertson. *Understanding how forensic science may contribute to miscarriages of justice*. Taylor & Francis, 2013.

- [90] J. Robins. ‘Explosive’ report into Danny Major case could result in criminal charges, 2016. Retrieved 29 Jan 2021 from: <https://www.thejusticegap.com/12548/>.
- [91] J. Roper. The true hell of the Post Office Horizon scandal, 2020. Retrieved 16 Feb 2021 from: <https://www.conveniencestore.co.uk/your-stories/the-true-hell-of-the-post-office-horizon-scandal/602552.article>.
- [92] K. Rossmo. *Criminal Investigative Failures*. CRC Press, 2008.
- [93] Royal Mail Group. Investigations, Prosecutions and Security in the Royal Mail A Brief History, 2010. Retrieved 14 Dec 2020 from: https://www.whatdotheyknow.com/request/post_office_investigation_branch_2#incoming-73875.
- [94] N. Ryder. The Re-invention of the Post Office? *Business Law Review*, 22(8/9):193–197, 2001.
- [95] M. J. Saks, D. Risinger, R. Rosenthal, and W. C. Thompson. Context effects in forensic science: A review and application of the science of science to crime laboratory practice in the United States. *Science & Justice*, 43(2):77–90, 2003.
- [96] R. Salet and J. Terpstra. Critical review in criminal investigation: evaluation of a measure to prevent tunnel vision. *Policing: A Journal of Policy and Practice*, 8(1):43–50, 2014.
- [97] H. Salim and S. Madnick. Cyber safety: A systems theory approach to managing cyber security risks—Applied to TJX cyber attack. *Work. Pap. CISL 2016*, 9:81–110, 2016.
- [98] H. M. Salim. Cyber safety: A systems thinking and systems theory approach to managing cyber security risks. Master’s thesis, Sloan School of Management, the School of Engineering, and the Department of Electrical Engineering & Computer Science, 2014.
- [99] Second Sight. Initial Complaint Review and Mediation Scheme, 2015. Retrieved 2 Jan 2021 from: https://www.jfsa.org.uk/uploads/5/4/3/1/54312921/report_9th_april_2016.pdf.
- [100] D. E. Shelton. Forensic Science Evidence and Miscarriages of Justice. In X. Mallett, T. Blythe, and R. Berry, editors, *Advances in Forensic Human Identification*, chapter 19. CRC Press, 2014.
- [101] Sky News. Post office won’t block appeals of 44 wrongfully convicted horizon scandal postmasters, 2020. Retrieved 15 Feb 2021 from: <https://news.sky.com/story/post-office-wont-block-appeals-of-33-wrongfully-convicted-horizon-scandal-postmasters-12087598>.
- [102] J. Slingo. Post Office IT contractor faces prosecution after judge’s ‘grave concerns’ about evidence, 2019. Retrieved 14 Feb 2021 from: <https://www.lawgazette.co.uk/news/post-office-it-contractor-faces-prosecution-after-judges-grave-concerns-about-evidence/5102540.article>.
- [103] L. Smalarz, S. Madon, Y. Yang, M. Gyll, and S. Buck. The perfect match: Do criminal stereotypes bias forensic evidence analysis? *Law and Human Behavior*, 40(4):420–429, 2016.
- [104] J. Smith. I’m amazed at the Dando verdict. Aren’t you?, 2001. <https://www.independent.co.uk/voices/commentators/joan-smith/joan-smith-im-amazed-at-the-dando-verdict-arent-you-9148148.html> Retrieved 3 July 2020.
- [105] N. Smith. Jill Dando: how pressure to find a killer made the criminal justice system reckless, 2019. Retrieved 29 Jan 2021 from: <https://www.thejusticegap.com/jill-dando-how-pressure-to-find-a-killer-made-the-criminal-justice-system-reckless/>.
- [106] Y. Song. *Applying system-theoretic accident model and processes (STAMP) to hazard analysis*. PhD thesis, Department of Computing & Software Engineering, 2012.
- [107] D. J. Soroach. Wrongful convictions: preventing miscarriages of justice some case studies. *Tex. Tech L. Rev.*, 41:93–116, 2008.
- [108] J. Spires. Police pay couple £200,000 after false accusation of flying drone at Gatwick, 2020. Retrieved 29 Jan 2021 from: <https://dronedj.com/2020/06/16/police-pay-couple-200000-accused-of-flying-drone-at-gatwick/>.

- [109] Stage 1 hearing session: transcript. Stage 1 hearing session: ‘hearing from those affected’ - 15 January 2021 open focus group session 001, 2021. Retrieved 16 Feb 2021 from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/961552/horizon-transcription-jan-2021.pdf.
- [110] N. Sunde and I. E. Dror. Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. *Digital Investigation*, 29:101–108, 2019.
- [111] The Arthur Conan Doyle Encyclopedia. George Edalji, 2019. Retrieved 17 Feb 2021 from: https://www.arthur-conan-doyle.com/index.php/George_Edalji.
- [112] The Associated Press. Chief Justice notes Kavanaugh case, cites dangers of “political pressure”, 2018. Retrieved 31 Jan 2021 from: <https://www.cbsnews.com/news/john-roberts-chief-justice-stresses-independence-minnesota-speech/>.
- [113] The Honourable Justice Fraser. Judgment (No.3) “Common Issues” Case No: HQ16X01238, 2019. Retrieved 14 Feb 2021 from: <https://www.judiciary.uk/wp-content/uploads/2019/12/bates-v-post-office-judgment-no3-15-mar-19.pdf>.
- [114] The Honourable Justice Fraser. Judgment (No.6) “Horizon Issues” Case No: HQ16X01238, HQ17X02637 and HQ17X04248, 2019. Retrieved 14 Feb 2021 from: <https://www.judiciary.uk/wp-content/uploads/2019/12/bates-v-post-office-judgment.pdf>.
- [115] The Postal Museum. The Post Office Investigation Branch, 2019. Retrieved 14 Dec 2020 from: <https://www.postalmuseum.org/blog/the-post-office-investigation-branch/>.
- [116] UNITED NATIONS. The Universal Declaration of Human Rights, 1948. Retrieved 5 June 2020 from: <https://www.ohchr.org/EN/UDHR/Pages/UDHRIndex.aspx>.
- [117] G. Usher. UK commentary: The Guildford Four: English justice and the Irish community. *Race & Class*, 31(3):81–98, 1990.
- [118] M. Van der Bruggen and A. Grubb. A review of the literature relating to rape victim blaming: An analysis of the impact of observer and victim characteristics on attribution of blame in rape cases. *Aggression and Violent Behavior*, 19(5):523–531, 2014.
- [119] J. Walker. Post Office Horizons scandal branded ‘largest miscarriage of justice in our history’, 2020. Retrieved 16 Feb 2021 from: <https://www.chroniclelive.co.uk/news/north-east-news/post-office-horizons-scandal-branded-18396679> Retrieved 3 Jan 2021.
- [120] N. Wallis. Post Office vs Mental Health: “It’s been a living hell”, 2019. Retrieved 2 January 2021 from: <https://www.postofficetrial.com/2019/08/post-office-vs-mental-health-its-been.html>.
- [121] N. Wallis. The Post Office Trial: Common issues trial judgement cheat sheet, 2019. Retrieved 03 April 2020 from: <https://www.postofficetrial.com/2019/04/common-issues-trial-judgment-cheat-sheet.html>.
- [122] WhatDoTheyKnow. Post Office Limited Horizon System, 2011. Retrieved 16 Feb 2021 from: https://www.whatdotheyknow.com/request/post_office_limited_horizon_syst.
- [123] M. Wilkinson, N. Pisa, and A. Bennett. Man arrested with wife over Gatwick drone chaos described as ‘expert flier’, 2018. Retrieved 30 Jan 2021 from: <https://www.thesun.co.uk/news/8046924/gatwick-drone-updates-man-arrested-wife-flier/>.
- [124] B. Woffind. *The Nicolas Cases. Casualties of Justice*. Bojangles Books, Cornwall, UK, 2016.
- [125] www.parliament.uk. Private prosecutions: safeguards, 2020. Retrieved 14 Dec 2020 from: <https://publications.parliament.uk/pa/cm5801/cmselect/cmjust/497/49704.htm>.
- [126] M. Zappala, A. L. Reed, A. Beltrani, P. A. Zapf, and R. K. Otto. Anything you can do, I can do better: Bias awareness in forensic evaluators. *Journal of Forensic Psychology Research and Practice*, 18(1):45–56, 2018.

A Appendix (Expert Evaluation)

Preamble

We have come up with an extension of an existing framework called FORZA (proposed by Jeong [49]). The aim of the extension is to neutralise the kinds of human bias that can lead investigators to rely on a single source of information, and then to ignore subsequent evidence which might point to another cause. In the table below, you will see the measure we suggest for achieving this during each of FORZA's investigation stages.

PRECEPT-4-Justice Details

Here Table 2 is provided.

Questions

Now, please answer the following questions:

1. Is the framework extension self explanatory?
2. Are the framework's proposed mitigations understandable?
3. If not – (a) what is not clear, (b) what could be improved?
4. Does the suggested process align with your understanding of *objective* digital forensics investigations?
5. In your opinion, would the application of the PRECEPT-4-Justice framework potentially have provided a different outcome in the Post Office case?
6. Please comment on the proposed extensions to the FORZA framework (use table below).
7. Any further comments or suggestions for improvement are very welcome

Here, Table 3 is provided to collect feedback.

B Evaluation Expert Quotes

The expert evaluators made the following suggestions (Evaluator i referred to as Ei):

1. Conceptual Investigation -

- (a) *Need for formulating hypotheses at outset*: E2 considers that generating hypotheses from the outset would engender bias. Rather identify different lines of enquiry and the reasoning behind it, that includes the exculpatory path.
- (b) *Need for multiple investigators*: There is no need to have a different person for each stage of the investigation as long as the investigation adheres to the current procedure, is supervised and controlled throughout and the final decision to prosecute is made by an independent body based on the evidence presented to them eg CPS. (E4); The word multiple is used what is the definition of multiple and how many would be acceptable. The investigator should independently look for a reason why something has happened etc and attempt to negate this or prove it has happened whether this is in favour of the prosecution or the defence. Therefore generating hypotheses should be on the fly as the investigation proceeds and not generated in a list at the beginning of the investigation. Actions should be raised by the supervisor of the case to investigate hypotheses that come to light (E4). The framework needs examples of multiple hypotheses (E9).
- (c) *Resourcing Issues*: Resourcing issues with multiple investigators (E2); Would this not add significant burden (time/ resources)? (E5); Yes, at increase cost and time (I know, justice v time argument) and an independent investigation; (E7) Resource constraints may prevent this from happening (E8); Overall, this would seem to be a rather resource-intensive exercise. Would any organisation have the means to pull this off? In South Africa, for example, we had one investigating officer who had numerous case dockets concurrently opened and she was the ONLY officer dealing with it. Ethically, an investigator owes it to the parties involved to carry out a thorough investigation but whether that is realistically achievable may be an even bigger challenge (E8). Three separate individuals is ideal, but often budgets don't all for this. Additionally, understanding the analysis from another forensic examiner is not straightforward. Maybe a more realistic option is a review of findings from another investigator? Same budget problem, but maintains the coherence between examination, analysis and reporting (E9).

Table 2: Adding a human bias dimension to FORZA (RC=Root Cause)

Level	Possible Bias	RC	PRECEPT-4-Justice Mitigation Measure
Conceptual investigation:	Bias 5, Bias 6	RC1, RC4	Hypothesis Generation: Generate multiple and competing hypotheses [88] to deliberately mitigate against a tendency to tunnel vision. Assign different hypotheses to different investigators [47].
Contextual Layer:	Bias 1	RC1	Appoint and Inform Case Manager: Ensure that the case manager is aware of all the information related to the case [23]. Rossmo [92] argues that the case leader has a key role in shepherding the investigation and ensuring that investigators do not engage in tunnel vision.
Legal Advisory Layer:	Bias 3, Bias 6	RC1, RC4	Guarantee Independence of Investigators: Ensure that digital investigators are independent and have no conflicts of interests. Indeed, demonstrating independence is an essential obligation in internal investigations [10]. Bigler <i>et al.</i> suggest that the forensic expert, investigator and author of the final report be three different and independent people. They also argue that if investigators/forensics experts/authors are employees of the company who instigates the investigation, they have to provide a statement explaining how they ensured their independence throughout the process.
Conceptual Security Layer:	Bias 8		Software Security Assurances: Examine information security processes. Marshall <i>et al.</i> [65] argue that the organisation’s information security standards and processes be examined. They should report on the relevant penetration tests that have been carried out to ensure that software vulnerabilities have been removed.
Technical Preparation Layer:	Bias 6	RC1, RC4	Validate Software Error Detection and Correction: Examine error and maintenance log to see which errors were reported and how they were addressed. Marshall <i>et al.</i> [65] argue that computer bugs <i>must</i> be fully disclosed. They should report on the relevant audits that have been carried out to ensure that standards have been adhered to. Finally, they should be required to provide evidence of error reports and system changes and be able to demonstrate that they have implemented measures which can detect malfunctioning software.
Data Acquisition Layer:	Bias 4	RC3, RC4, RC5	Acquire evidence using two different tools: Ensure that all digital evidence has been gathered and is considered as part of the investigation. Acquisition should take place according to the appropriate legal guidelines. At least 2 different digital forensics software tools should be used to acquire data [1, 9, 25]. The “raw” data before acquisition should be made available to 3rd party (defence).
Data Analysis Layer:	Bias 2, Bias 6	RC1, RC2, RC3, RC4	Construct timeline for each hypothesis: Refer back to the investigation layer, and extract information that could potentially prove critical for proving each of the multiple hypotheses. Attempt to reconstruct a timeline for each of the hypotheses. Investigators should deliberately play devil’s advocate and continuously strive for objectivity [92].
Legal Presentation Layer:	Bias 4	RC3, RC4, RC5	Compose reports for each competing hypothesis: Reports should be written by independent investigators. They should then meet to argue their different explanations for the events that triggered the investigation [47]. All processes used, and all results identified in data analysis should be provided in full disclosure. Ensure that the case is made for and against competing hypotheses is presented, and backed up with corroborated evidence i.e. not only software generated evidence.

Table 3: Expert evaluation questions

	How realistic is the proposed mitigation in PRECEPT-4-Justice?	Suggestions for Refinement? (Table 2)
Ability to Offset Confirmation Bias Tendencies		
Ability to offset tendencies to assume guilt		
Ability to Neutralise Toxic Institution Culture compromising investigation independence		
Ability to Assure Investigator Independence of		
Ability to detect any possible software bugs/security issues		
Ability to carry out an objective investigation		

- (d) *Need for investigator training:* Regular training in Bias Elimination for the whole investigation team (E3); The examiners should be proficient in the collection, retention, processing and analysis of digital data. A thorough review of the software prior to interviews would have been of paramount importance. (E1).
- (e) *Should internal investigations be permitted without external oversight?:* More emphasis on the use of third party forensic investigators (E1).
- (f) *Hypothesis quality:* Hypotheses need to be demonstrably exhaustive & mutually exclusive (E3).

2. Contextual Layer:

- (a) *Case Manager should be external:* Potential to also ensure the case manager is from outside the organisation to maintain the independence (E6).
- (b) *Case Manager's Role:* Time may be a factor, or team members who deem themselves highly experienced and shut down the opinions of others (E8).

3. Legal Advisory Layer

- (a) *Need for external investigator:* Should at least one external investigator be part of this process to avoid collusion and evidence destruction? (E5) Since this framework is only looking at internal investigators – the consideration of whistle-blowing process should be considered for employees to report concerns / information (Public Disclosure Act 1998) (E5).
- (b) The legal advisory layer could benefit from mentioning separation of duties as a security baseline.
- (c) *Investigator Independence:* Eliminate any systemic pressures to 'get a conviction' (E3).

4. Conceptual Security Layer

- (a) *Context of Event:* What about consideration of board decision to invest or reject investment into technical solutions, upgrades, training – mitigation for lapse in security (E5).
- (b) *Verification of Software Security:* It may be beneficial to include examples of security standards which could be adhered to, which will validate the Conceptual Security Layer (E6).

5. Technical Preparation Layer:

- (a) *Verification of Software:* Evidence of a secure development lifecycle and potential of multiple vulnerability management solutions would mitigate this (E6). Finding exculpatory evidence is key but even harder when it relies on software testing. Explain how software testing ought to be carried out (E7). Leave the detection, mitigation, and remediation of software bugs to other frameworks (E9).

6. Data Acquisition Layer:

- (a) Would it not be far safer to provide images (unless that is what you meant) (E5);
- (b) *Chain of custody:* Potential to mention chain of custody of evidence within the data acquisition and legal presentation layers (E6).

- (c) *Audit Trail*: All exculpatory evidence must be declared (E2).
- (d) *Using more than one forensic tool*: Is using 2 software tools sufficient to guarantee this beyond a reasonable doubt? (E3) Using two different tools may or may not be feasible or useful. For example, it's unlikely that using FTK and Encore would result in meaningful differences. That said, I like the idea of verification across more than one tool. Describe a scenario where this is useful (E9); To acquire an image using 2 methods is time consuming and not necessary as long as the software used for the acquisition has been validated for use. Many of the acquisitions that I currently do take 5 to 10 days to have to do them twice would not be practical (E4); Obviously, the use of dual-method or dual-tool verification should be essential however, it does not ensure quality assurance. For example, both tools may share the same libraries etc. and hence the same results. I think it is just worth noting that dual-tool verification does not eliminate biases or assure quality (E10).

7. Data Analysis Layer:

- 8. **Legal Presentation Layer:** The defence should be given a copy of the acquired evidence as was used by the investigator (E4).
- 9. **Cross Cutting:** Keep decision log (E2). If you encounter something that runs counter to your evidence, that has to be investigated and noted in exculpatory evidence (E2).

10. Limitations:

- (a) If the organisation is left to investigate this [Framework] would still not be entirely result in independent outcomes (E7). I don't think any framework or tool will be capable of neutralizing a toxic culture. A strong leader combined with a coordinated management team seems to be the only viable method of altering or improving a toxic org culture (E9).
- (b) All of the proposed extension will not be easy to mitigate as they all deal with the individual investigator and therefore will be subject to human nature. Having said that the following will go some way to achieving this (E4) i.e. (1) Qualifications and training of investigator, (2) Code of ethics for investigators, (3) Membership of professional body, (4) Good standing within professional body to be an investigator, (5) Requalification exams annually, (6) Work for a forensic investigation practice and perform investigations using proven investigative methodologies and tools, (7) Investigations dip sampled and checked by professional body
- (c) I don't believe we have to go to this length in some of the sections and current policies and procedures in place are sufficient if they are followed. For example the software which the evidence was relied upon was not trusted and tested forensic software but an operational program. Faults were known but not disclosed in the case. This is contrary to the procedures we have in place now in relation to disclosure. (E4)

- 11. **Future Work:** Perhaps this can be evolved and extended to provide "best practices" in carrying out each task. Things like team composition may be useful (mixing levels of seniority / experience in a particular type of investigation / skillset mix) (E8)