

The Development and Validation of the Social Media Surveillance Scale (SMSS)

Alice Thompson

PhD Researcher, Psychology

PECC 2026

What is Online Surveillance?

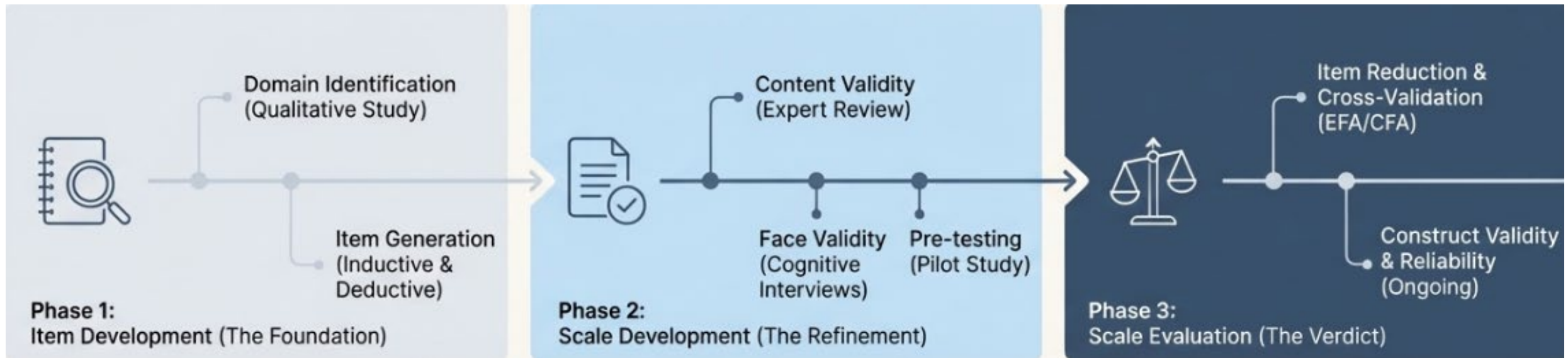
- Social media = connection, maintain relationships, belongingness (Kuss & Griffiths, 2011)
- Problematic, Preoccupation & Disinhibited (Acquisti, Brandimarte, & Loewenstein., 2020)
- Social Media propelled individuals into a surveillance culture, promoting observant actions and stalking mentalities (Lyon, 2017).
- “Creeping, Lurking, Online Monitoring, Electronic Surveillance, Information Seeking, Cyberstalking”



The Research Gap

- Existing scales often focus narrowly on extreme behaviours (e.g., cyberstalking)
- Neglecting the wide spectrum of everyday surveillance.
- Creates a knowledge gap on how normalised online behaviours (e.g., Creeping) can escalate into deviance.
- Without a measure, it is difficult to investigate.

A Multi-Phase Journey from Concept to Validated Scale

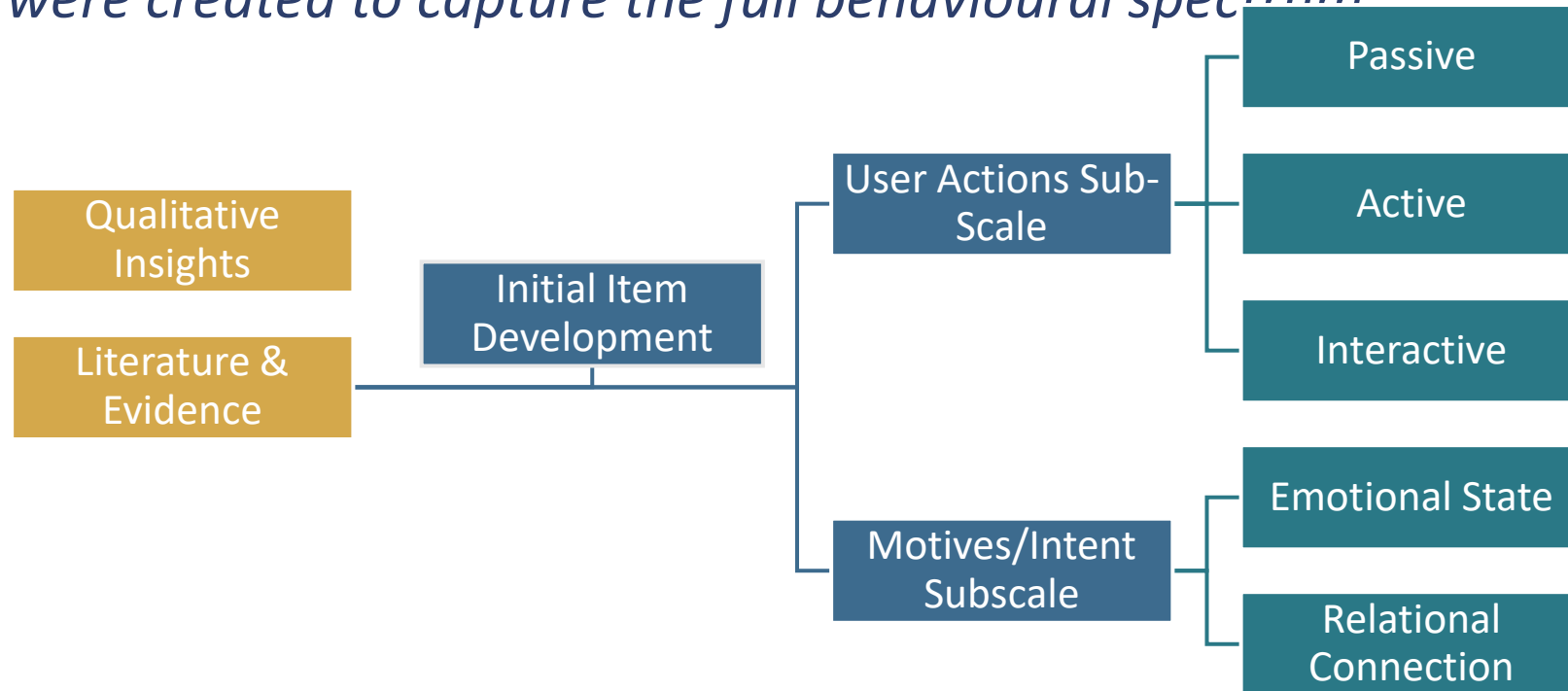


Laying the Foundation (Item Development)

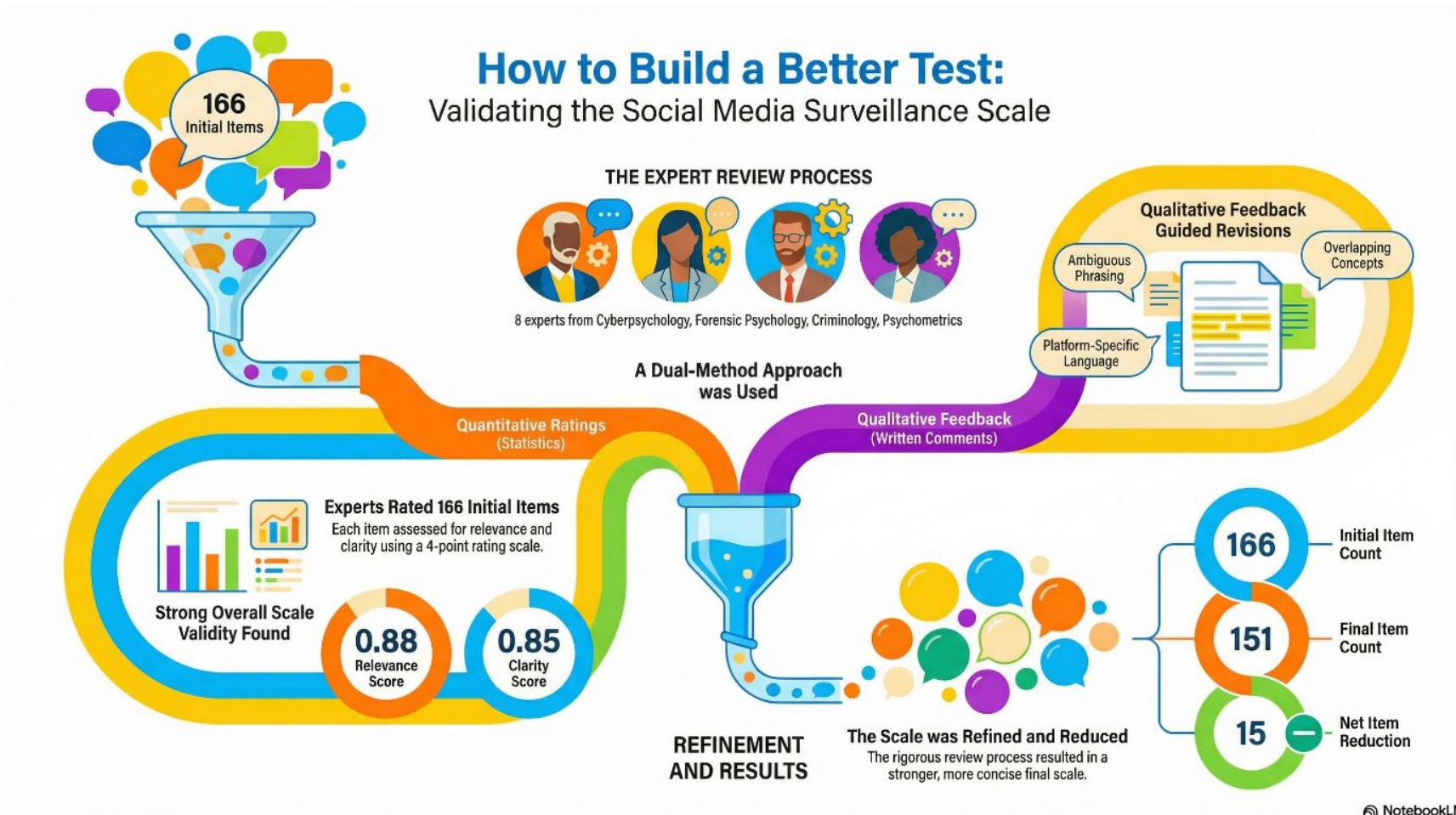
Part 1: Inductive Approach (Qualitative Study)

Part 2: Deductive Approach (Literature Review)

166 items were created to capture the full behavioural spectrum



Content Validity: *Expert Review Process*



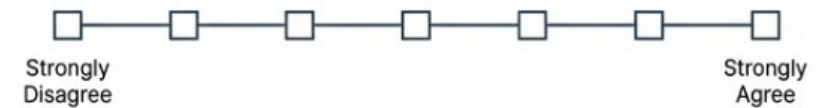
Face Validity: *Cognitive Interviews*

Process

- *Aim:* Evaluate face validity; whether items are understandable and appear relevant to non-experts **168 initial items**
- *Method:* 12 participants individual cognitive interviews; a technique used to evaluate interpretability of scale items. **151 items retained post expert review**
- *Techniques used:* ‘Think aloud’ exercises, paraphrasing, comprehension and general probes. **113 items retained post cognitive interviews**
- *Analysis:* d’Ardenne and Collins (2015) cognitive framework of survey responding.
- *Outcome:*
 - Feedback led to key revisions for clarity and inclusivity or deletion of items.
 - E.g., Wording was refined, “browse” changed to “scroll”

Pilot Study: *Pretesting items*

Endpoints-Only Version



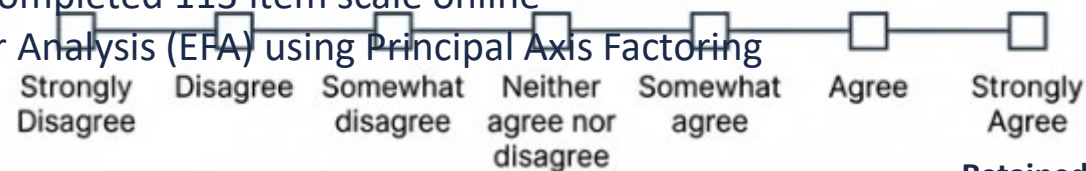
Purpose: To compare two versions of 7-point Likert scale; one with every point labelled, and one with only endpoints labelled.

Method:

- 307 participants completed 113 item scale online
- Exploratory Factor Analysis (EFA) using Principal Axis Factoring

Results:

Fully Labelled Version



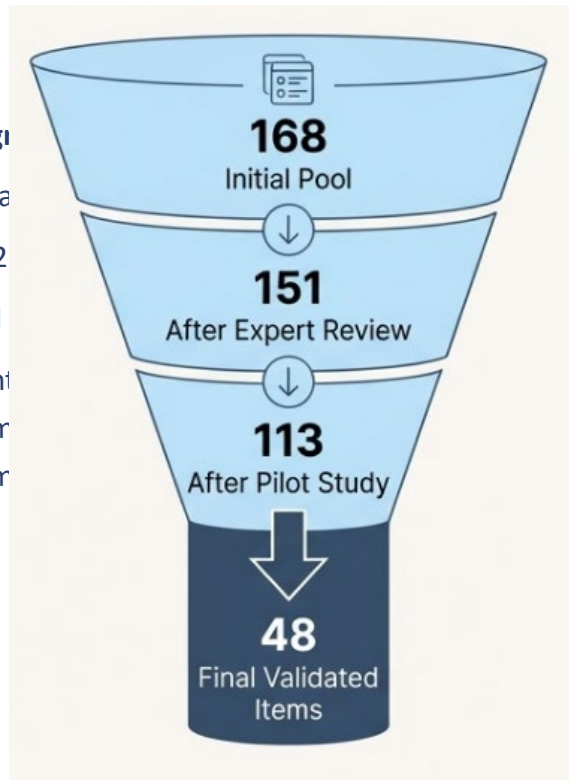
Group	Format	N	KMO	Factors	Variance	Retained Model
A	Labelled	172	.75	6	45.7%	✔ Six-factor
B	Unlabelled	135	.64	5	46.3%	—

Decision: The labelled version produced more distinct constructs and was selected for full evaluation.

Scale Evaluation: *Item Reduction and Cross-Validation*

Sample and Design

- N = 1,641 social
- Mean age = 42
- Data screened
- Sample split into
 - Subsam
 - Subsam



es
/
duplex:

Model Comparison					
Model	χ^2 (df)	CFI	TLI	RMSEA [90% CI]	Decision
5-Factor	43,439 (2,773)	.36	.35	.13 [.13–.14]	Poor fit
6-Factor	11,347 (1,065)	.98	.98	.11 [.11–.12]	Retained

Scale Evaluation: *Item Reduction and Cross-Validation*

Connective Behaviours



Affiliative Social Interaction

Positive, prosocial actions used to connect and maintain existing relationships.

Example Actions: Liking posts, leaving positive comments, and replying to friends' stories.



Relational Following

Monitoring people you know to feel reassured about your social connections.

Example Actions: Following friends, family, or romantic interests you have met in person.



Preoccupied Engagement

Emotionally driven attempts to gain attention or a reaction from a specific person.

Example Action: Excessively messaging or liking someone's content to get them to notice you.

Intrusive Behaviours



Investigative Searching

Deliberate and effortful searching across platforms to gather information on someone.

Example Action: Thoroughly searching through a person's followers, posts, and multiple profiles.



Deceptive Monitoring

Using fake or anonymous profiles to observe someone without their knowledge.

Example Action: Creating a fake account to check up on specific people.



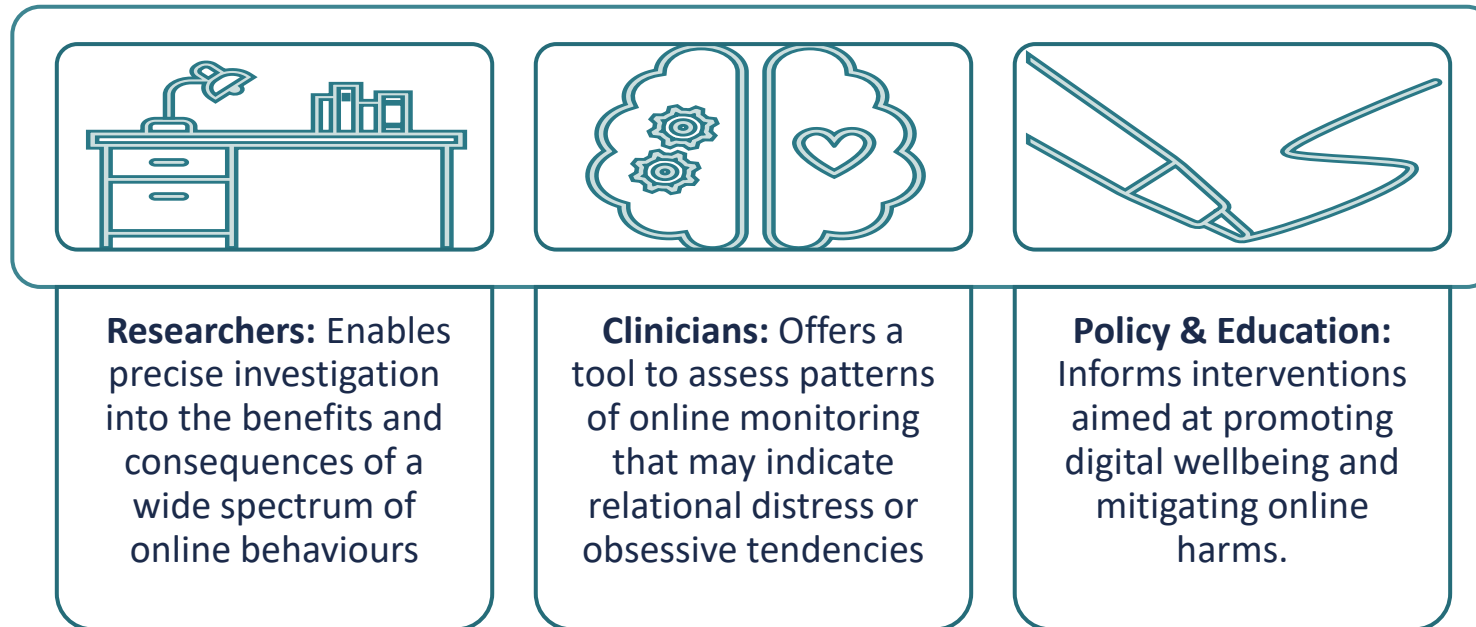
Privacy Intrusion (Digital Violation)

Accessing someone's private account, messages, or device without their permission.

Example Action: Logging into a partner's social media account to monitor their activity.

Phase 3 to complete!

- Scale Evaluation: *Construct Validity (Ongoing)*
- Contribution...



Thank you for listening!

