PRIVACY IN POLICE DIGITAL FORENSIC INVESTIGATIONS

"What are the intelligence and investigative gaps?"

Paul van Schaik[1*], Alastair Irons[3], Karen Renaud[2,3]

[1]Teesside University, [2]University of Strathclyde,
[3]Abertay University *p.van-schaik@tees.ac.uk

Outline

- Background
- Interview study
- Method
- Results
- Potential implications
- Discussion
- Conclusions

Background

Individual Privacy

Society at Large

Use privacy-enhancing tools (PETs)

hinder police digital forensic (DF) investigations

Privacy should be taken into consideration during any police DF investigation.

PRECEPT: a framework for ethical digital forensics investigations

R.I. Ferguson
Division of Cyber Security, Abertay University, Dundee, UK
Karen Renaud
Division of Cyber Security, Abertay University, Dundee, UK; Rhodes University, Grahamstown, South Africa and University of South Africa, Pretoria, South Africa
Sara Wilford
Centre for Computing and Social Responsibility, De Montfort University, Leicester, England, and
Alastair Irons
University of Sunderland, Sunderland, UK

Received 13 May 2019
Revised 1 October 2019
2 December 2019
Accepted 2 December 2019

- Theoretical analysis rather than of stakeholders' perceptions
- PET use by the general public not addressed
- Trade-offs between security and privacy not addressed

AIM:

Identify aspects of privacy and PET use that inform or affect DF investigations

RESEARCH QUESTIONS:

How do considerations of privacy and PET use inform or affect DF investigation?

What are police stakeholders' perceptions of PET use by citizens?

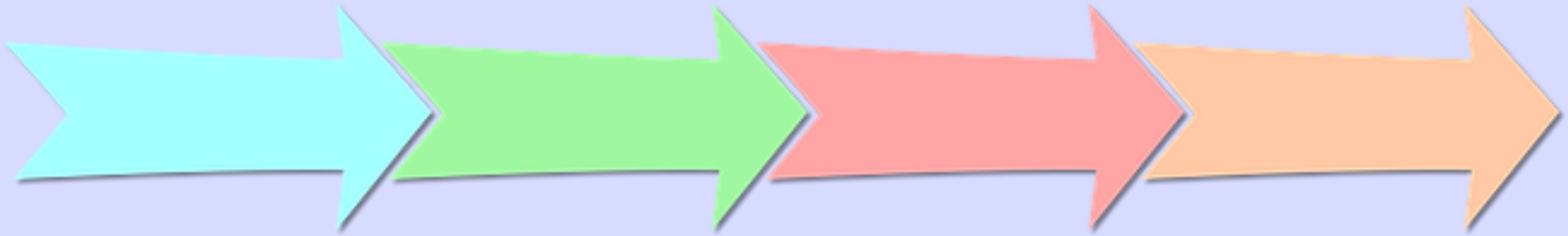
PARTICIPANTS

- **Semi-structured interviews**
- **Sample: police DF investigators from a range of UK forces**
  - DF lab managers
  - DF investigators
- **Includes DF units of two large police forces**

N = 8

PROCEDURE

- Semi-structured interview guide
- Privacy-related PRECEPt principles (11 in total): how does each inform DF investigation?
- How does citizens' use of PETs affect DF investigation?



Data analysis

- Thematic analysis
- Deductive coding: by PRECEPt principle
- Inductive coding: themes that do not naturally match PRECEPt principles
- Results on the following slides

Privacy Principles

Ferguson *et al.* (2020)

P1	Consent and choice	P7	Openness, transparency and notice
P2	Purpose legitimacy and specification	P8	Individual participation and access
P3	Collection limitation	P9	Accountability
P4	Data minimization	P10	Information security controls
P5	Use, retention and disclosure limitation	P11	Compliance
P6	Accuracy and quality		

☑ YES
☒ NO

TIMELINESS OF DF EXAMINATION WORK

- (Iterative) redrafting of DF examination request
- Process automation of aspects of DF examination jobs
- (Lack of) DF capacity
- Increased volume of DF examination jobs

PRIVACY-ENHANCING TECHNOLOGY USE BY CITIZENS

- Benefits of PETs and disadvantages for DF examination
- Default PETs and citizens' awareness
- Approaches to access 'protected' evidence
- Proportionality - attempt at 'breaking' PETs depends on seriousness of the offence
- Cloud storage of exhibits; PET 'arms race'; PET types
- Potential implications on following slides

P01 CONSENT AND CHOICE

Suspect

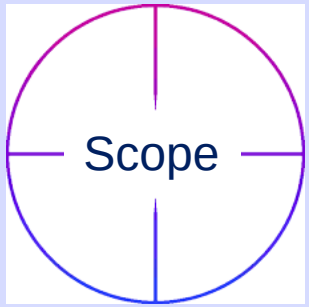
Victim

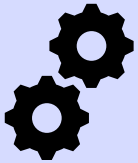
Witness

Respect
Rights
&
Wellbe**ing**

DF Investigator

P02 Purpose legitimacy and specification

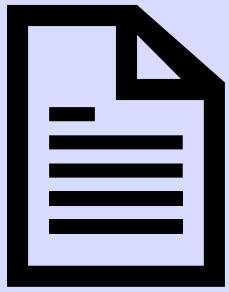




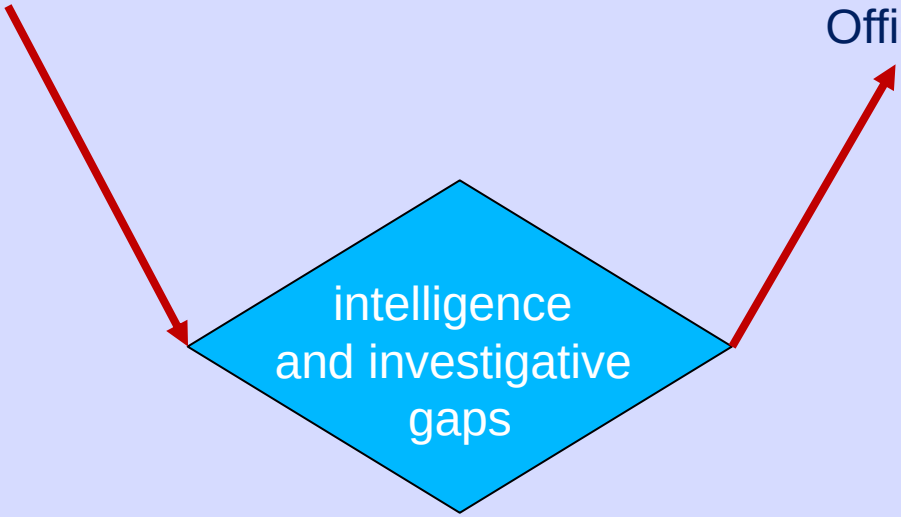
Tools

DF Investigator

Investigating Officer



Guidelines



Potential implications for DF investigation

P03 Collection limitation

Have a system for internal as well as external oversight of DF examination in place

P06 Accuracy and quality

Consider using automation where appropriate for accurate consistency and speed

Potential implications for DF investigation

P09 Accountability

Record the examination process and justify decision-making

Consider industry standard accreditation for audit trail

P11 Compliance

Consider industry standard accreditation for compliance

Standardisation of DF examination process across police forces could provide **equity** across the country

Potential implications for DF investigation

Theme: Timeliness of DF examination work

Consider basic training to improve

(a) communication between investigating officers and DF teams, and

(b) reduce the need for redrafting examination requests,

thereby increasing the speed and quality of investigation

Theme: Privacy-enhancing technology use by citizens

Encourage citizens to protect themselves online in order reduce the volume of digital-related or digital-enabled crime

Potential implications for DF investigation

- **Specific links to Police Foundation's 2022 report: regarding future skills**
  - Future trend: greater need to work within an ethical framework online
  - Skills requirement: understanding of ethical issues
  - Recommendation: 'a significant investment in digital forensics'

Discussion

Previous work focused on forensics more generally (including DF) or DF only, but not exclusively on privacy in relation to DF

House of Lords (2019)

> "We see a clear benefit in ensuring that most forensic science providers are accredited to the *appropriate* [emphasis added] ISO standards. The Forensic Science Regulator should review the current regulation framework and make any necessary changes to ensure that it promotes good practice."

House of Lords (2019)

"… legal practitioners can make unrealistic demands of the police and digital forensic examiners due to a lack of understanding of digital evidence. The CPS does not always understand police technical capabilities, whether that is due to resource constraints or outdated equipment."

Muir and Walcott (2021)

"… when we spoke to digital forensics specialists they told us of the need for much better training and awareness of digital forensic techniques among the general workforce, so that officers can be much more intelligent users of specialist services."

Discussion (2)

More links with previous work

Muir and Walcott (2021)

> "There is a need for much clearer national guidance for police officers regarding the examination of digital evidence. We suggest that there should be minimal intrusion relative to the needs of the investigation."
>
> "Training in digital forensics should be provided for all practitioners in the criminal law, including judges, prosecutors and defence barristers."
>
> "The College of Policing should issue clearer guidance regarding the use of powers to extract cloud data."
>
> "National data retention policies should be reviewed, and clear guidance issued clarifying when deletion is appropriate."

Discussion (3)

More links with previous work

Police Foundation (2022)

‘Digital forensics in particular has “woeful levels of compliance with achieving quality standards”. The ultimate upshot of this is misleading evidence (Smit et al., 2018), long backlogs, innocent people being falsely convicted and criminals escaping justice (Tully, cited in Dodd, 2020).’

“Digital intelligence and investigation training should be incorporated into minimum professional standards regulated by the College of Policing.”

“A national police workforce planning unit should be established within the College of Policing to project future [DF] demand, monitor current and future skill gaps and coordinate a national response.”

Conclusions

- **High-level question/aim**
  - How to reconcile the security requirements of society at large with the right to privacy of individual citizens?
  - Analyse stakeholders' perceptions
- **Analysed privacy in police DF investigations**
- **Identified**
  - specific uses of privacy-related principles in DF investigation
  - issues for DF investigation from citizens' use of PETs
  - potential implications for practice