Privacy in UK Police Digital Forensics Investigations

Paul van Schaik
Teesside University, UK
p.van-schaik@tees.ac.uk

Alastair Irons
Abertay University, Scotland
a.irons@abertay.ac.uk

Karen V. Renaud
Strathclyde University, Scotland
University of South Africa
Abertay University, Scotland
Rhodes University, South Africa
karen.renaud@strath.ac.uk

Abstract

Background: *Privacy is a human right, but what happens when a person's privacy rights encounter legitimate police investigations? Is it even possible to carry out these investigations in a privacy-respecting way? If the person being investigated makes use of privacy-enhancing technologies (PETs), how does this impact digital forensics investigations?*

Aim: *The aim of our study was to identify how privacy rights and the use of PETs influence police digital forensics practices.*

Methods: *We carried out a study with 10 digital forensics investigators from UK police forces to explore how considerations of privacy and citizens' PET use inform or affect digital forensics investigations.*

Results: *We identified specific uses of privacy-related principles that ought to apply in digital forensics investigation, and hindraces to digital forensics investigations from citizens' use of PETs.*

Conclusions: *We concluded with potential implications for practice and ideas for future research to reconcile the law enforcement activities with individual citizens' inalienable privacy rights.*

Keywords: police, privacy-enhancing technologies (PETs), digital forensics

1. Introduction

Privacy is the universal human right to consent before personal information is collected, stored and processed [European Convention, 2012]. Many countries have specific laws to protect the privacy of their citizens (Table 2 in Appendix A). Yet, the 21st-century citizen is under surveillance much more often than they realise, and this often violates their privacy [Königs, 2022]. For example, in 2012, the number of CCTVs in London had reached 422,000 — one for every 14 people [McCahill and Norris, 2002]. Atlanta, USA, has 15.56 CCTV cameras per 1000 people. Citizens of developed countries are intensively surveilled [Königs, 2022]. Airports monitor passenger movements [Wu and Radke, 2011], government and private security cameras keep watch [Armstrong and Norris, 2020], mobile phone apps monitor activities and connections [Cohen et al., 2020], and collect very personal information [Chaker, 2017].

Citizens of many countries appear to support such surveillance in the name of security and crime prevention [Ziller and Helbling, 2021], or at least do not protest openly [Renaud et al., 2016]. Authorities might well violate privacy unacceptably as a consequence [Seyyar and Geradts, 2020]. Consider that when crimes occur, digital forensics investigations could also violate the privacy of victims and suspects [BBC, 2018b, Dehghantanha and Franke, 2014]. In the UK, for example, the police carried out forensics investigations on the smartphones of crime victims [BBC, 2018a, Carlo and Ferris, 2019] and of other devices without warrants [Weston, 2018], violating their privacy [BBC, 2018b]. As a consequence of the public outcry, the Digital Processing Notice (DPN) required police forces in England and Wales to obtain consent before searching any digital device belonging to a victim [HMICFRS, 2022]. The [College of Policing, 2021] also released a new set of guidelines for obtaining data from devices. One guideline is that consent ought not to be obtained by coercion, but a victim might still feel impelled to consent [Renaud et al., 2016]. In essence, digital forensics investigations should respect citizens'

URI: https://hdl.handle.net/10125/106617
978-0-9981331-7-1

privacy where practicable.

Citizens might use PETs to preserve their own privacy or to confound digital surveillance and digital forensics investigations [Ferguson et al., 2018]. In response, some governments have enacted laws to force people to divulge their encryption keys e.g., [BBC, 2018]. However, the extent to which PET usage has indeed deterred digital forensics investigations is unclear, hence this investigation. We explore the following questions:

RQ1: How do considerations of privacy inform or affect digital forensics investigations?

RQ2: What are police stakeholders' perceptions of PET usage by citizens?

Section 2 introduces privacy PETs and the impact of these on digital forensics investigations. Section 3 outlines our study, with Section 4 reporting on the findings and Section 5 presenting recommendations. Section 6 concludes.

2. Related Research

2.1. Privacy

Privacy is a human right in Europe, and the UK is a signatory of the European Convention of Human Rights. Article 8 of the Convention states [European Convention, 2012]: ***Right to respect for private and family life:***

(1) *Everyone has the right to respect for his private and family life, his home and his correspondence.*

(2) *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.* Privacy is also part of the Universal Declaration of Human Rights (Article 12) [United Nations, 1948], but this is sometimes not respected by those in authority [BBC, 2018a, O'Sullivan, 2020, Carlo and Ferris, 2019].

Many citizens do not object when their privacy rights are violated [Renaud et al., 2016]. [Gross, 1967] suggests that while people are often able to sense, intuitively, that their privacy is being violated, they struggle to articulate what privacy actually means to them, and are thus less able to insist that their privacy rights be respected. [Hart, 1983] explains that when it comes to privacy, people can 'know' what privacy is without being able to define the concept. Another possible explanation is advanced by [Bott and Renaud, 2018], who suggest that people have accepted the extensive and invisible privacy violations that occur when we are online, having gone through a grieving process and become resigned to the fact. Finally, it could simply be that preserving privacy is so arduous that people become fatigued and give up altogether [Van Der Schyff et al., 2023].

The ISO/IEC 29100:2011 standard [ISO, 2011] enumerates 11 privacy principles. We map these to other standard privacy principles in Table 1. It becomes clear that the ISO's is the most comprehensive list, which we shall use in this paper.

2.2. Digital Forensics

There is some awareness of the potential for law enforcement to respect the privacy of individuals they are investigating. For example, the Police Foundation [The Police Foundation, 2022] stresses the importance of privacy protection in police work but not specifically in relation to digital forensics. The Police Foundation also identified insufficient compliance with quality standards with negative consequences for outcomes of the judicial system. Privacy protection was not explicitly addressed in relation to digital forensics. The House of Lords [House of Lords, 2019] notes the benefit of ISO-standard accreditation by forensic science providers and concludes that "*there is a need for legal practitioners to develop a better understanding of what can be achieved by digital forensic evidence and in what realistic timescales*" (p. 5), but also does not address privacy protection in relation to forensic services. Also without analysing privacy specifically, [Muir and Walcott, 2021] also stress the need for better training and awareness regarding digital forensics among the police to ensure better use of digital forensics services. Furthermore, they recommend better guidance for police officers regarding how to examine digital evidence. They also recommend enhanced guidance regarding the legal basis for extracting data in cloud storage and regarding data retention.

Therefore, in this paper, we identify a lack of research on citizens' privacy during digital forensics investigations. Figure 1 shows how the ISO's privacy principles were mapped to digital forensics stages, as outlined by [Ferguson et al., 2020].

2.3. Privacy-Enhancing Technologies (PETs)

When it comes to authorities breaching privacy during digital forensics investigations [Ferguson et al., 2020], privacy can become a luxury [BBC, 2023]. We hasten to add that the majority of policemen and policewomen uphold standards of

Table 1. Alignment of Different Privacy Principles from the International Standards Organization [ISO, 2011], the Fair Information Practice Principles (FIP) [Landesberg et al., 1998], the Generally Accepted Privacy Principles (GAPP) [American Institute of Certified Public Accountants, 2010], the Organisation for Economic Co-operation and Development (OECD) [OECD, 2010], Global Privacy Standard (GPS) [Cavoukian, 2006]

ISO	FIP	GAPP	OECD	GPS
P1: Consent & choice.	Choice/ Consent	Choice and consent		Consent
P2: Purpose legitimacy and specification.			Purpose Specification	Purposes
P3: Collection Limitation.		Collection	Collection Limitation	Collection Limitation
P4: Data Minimization.				Data Minimization
P5: Use, retention and disclosure limitation.		Use, retention, and disposal	Use Limitation	Use, Retention, and Disclosure Limitation
P6: Accuracy and quality.		Quality	Data Quality	Accuracy
P7: Openness, transparency & notice.	Notice/ Awareness	Notice	Openness	Openness
P8: Individual participation and access.	Access/ Participation	Access	Individual Participation	Access
P9: Accountability		Management	Accountability	Accountability
P10: Information security controls.	Security/ Integrity	Security for privacy	Security Safeguards	Security
P11: Compliance.	Enforcement/ Redress	Monitoring and enforcement		Compliance

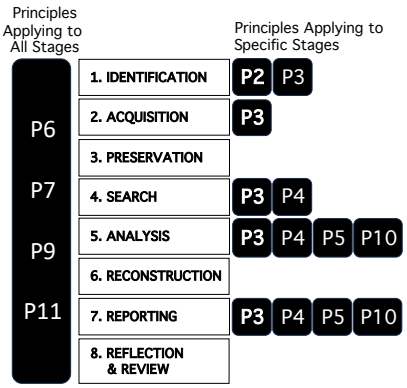

Figure 1. Digital Forensics Stages, Mapped to ISO's Privacy Principles (Pi) by [Ferguson et al., 2020]

integrity and would not violate the public's privacy in the course of their duties. However, there are some who do behave illegally, and PETs can protect people from such privacy-invasive actions. Nevertheless, the use of such technologies can also confound and interfere with legitimate digital forensics investigations. Therefore and given the importance of and lack of research on privacy in digital forensics, we chose to speak to digital forensics officers in the UK's police force, as a first step in exploring this domain.

Given that our focus is on privacy in the context of digital forensics, we will consider the kinds of PET that can confound or prevent digital forensics investigations [Ferguson et al., 2018]: **(1)** encryption [Casey et al., 2011], **(2)** full disk encryption using tools such as VeraCrypt or Bitlocker [Casey and Stellatos, 2008], **(3)** secure network communication using Virtual Private Networks [Conlan et al., 2016a], **(4)** secure processors [Irons and Lallie, 2014], **(5)** homomorphic encryption [Gentry, 2009] and **(6)** anonymous routing using TOR [Reed et al., 1998].

2.4. Segue into Study

Digital evidence is increasingly used in court cases [Reedy, 2020]. With respect to carrying out such investigations, there are two pertinent considerations. The *first* is related to the privacy rights of the person being investigated [Dehghantanha and Franke, 2014] i.e., how privacy considerations influence digital forensics investigations [Englbrecht and Pernul, 2020] —- *Consideration 1*.

The *second* is related to how deployed technologies can hinder investigations [Casino et al., 2022]. In particular, individuals being investigated might use PETs including [Conlan et al., 2016b, Centre for Data Ethics and Innovation, 2021]: *encryption*, *multi-party computation*, *differential privacy* and *remote wiping*. These could easily hamper the ability of the investigator to gather evidence —- *Consideration 2*.

With respect to ***Consideration 1*,** the House of Lords [House of Lords, 2019] said: "*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 regulatory framework and make any necessary changes to ensure that it promotes good practice." [Ferguson et al., 2020] applied the ISO/IEC 29100:2011 standard privacy principles to derive a set of ethical considerations to inform digital forensics investigations, showing that they can be fruitfully applied to this domain too. However, there is a lack of research analysing the extent to which these principles are applied *in practice* in digital forensics investigations.

With respect to ***Consideration 2*****,** every UK citizen has the right to privacy, and therefore the right to use PETs. However, police forces may then be unable to carry out digital forensics investigations. Ferguson *et al.* [Ferguson et al., 2018, p.53] explain that "*Encryption has thus reached the point of being "practically unbreakable"*. In essence, citizens, in protecting themselves from the activities of bad actors online by using PETs, also prevent government bodies from accessing their devices or listening in on their communications which they might legitimately need to do when carrying out investigations. Despite potential disadvantages for digital forensics investigation, there is little research analysing the extent to which citizens' use of PETs affects digital forensics investigations *in practice*. RQ1 and RQ2 align with these two considerations.

3. Study

We carried out semi-structured interviews to answer the two research questions presented Section 1. Since Ferguson *et al.*'s mapping of privacy principles to digital forensics stages was conceptual, we will consider all privacy principles in our investigation, not only those highlighted by Ferguson *et al.* in each stage.

This study is timely because there is a need to automate aspects of digital forensics examination jobs in the face of limited digital forensics capacity and increased volume of digital forensics examination jobs in the UK. Automation would have to be built in such a way that it respects privacy.

3.1. Research Design and Participants

We recruited UK digital forensics' investigators, digital forensics lab managers and digital forensics investigators, from a range of UK police forces. We wrote to every police force in the UK and also contacted our own professional and referred contacts. We interviewed those who responded. This included forensics units from two large UK police forces; we are not permitted to identify them. We conducted a series of 10 individual interviews using the interview protocol in the Appendix. We encouraged participants to provide relevant (anonymised) examples from their own and others' experiences.

3.2. Semi-Structured Interview Guide and Data Analysis

First, we presented the ISO's 11 privacy principles [ISO, 2011] (Table 1) to explore whether and how each informs digital forensics investigations. Second, the interviews explored how citizens' use of PETs affects digital forensics investigations. The interviews were conducted on VoIP and automatically transcribed. We then reviewed each transcript and returned it to the interviewee to review and remove any text before data analysis. We performed a thematic analysis [Braun and Clarke, 2006] with deductive coding by privacy principles. This was followed by inductive coding based on themes that did not naturally match ISO/ISEC 29100:2011 principles.

4. Findings

From our inductive coding, two new themes were derived. The first two subsections address RQ1 and the third subsection addresses RQ2. (PP*i* refers to Participant number *i*)

Timeliness of Digital Forensics Examinations

The timeliness of digital forensics examinations was either facilitated or hindered by the particular factors. Process automation of aspects of examination jobs sped up the process. This was enhanced by the possibility of running automated jobs around the clock rather than a regular 9-to-5 human work timetable. "*We'll forensically image everything that we get given to us so the automated process does a forensic image; it verifies the image. It then dumps that image file out into a digital forensics tool*" [PP6]. Examinations were slowed down by iterative redrafting of digital forensics examination requests. This happened in cases where the completed job request form did not meet the required standards. Examinations were delayed because of a lack of digital forensics capacity. This has also been highlighted in other recent work [Muir and Walcott, 2021]. Further delays occurred because of the increased volume of digital forensics examination tasks. This is because, as highlighted above, almost all examinations have a digital element. The resulting delays from these various causes of delay lead to concern in the criminal justice system: "*There has to be a focus on digital forensic service queues/backlogs and what that means for the investigation. Once a device is seized there may be a significant period between submission to a unit and the*

subsequent digital forensic report. More and more in the criminal justice system this is getting flagged as not acceptable" [PP5].

Privacy Principles

From deductive coding, the following insights were derived.

Principle 1: Consent and Choice: Conditions under which consent is/is not required and conditions under which seized devices are returned or destroyed were discussed. Demonstrating respect for human rights and protecting people's well-being was seen as important. With changes over time in the relevance of evidence, consent may need to be obtained once again. "*When a device has been taken voluntarily and the owner withdraws consent the examinations have to stop; this withdrawal is becoming more common; advice from the internal department: the information that had been extracted up to the point of withdrawal can still be analysed on a copy ('image') that can be taken before the device is returned, but no new information can be extracted without a warrant*" [PP3].

Principle 2: Purpose Legitimacy and Specification: Iterative redrafting of a digital forensics examination request is not uncommon. The request needs to be checked by a digital forensics investigator before the digital forensics examination can start, but the request form is not always of sufficient quality to allow this. Job submissions (enquiry request forms) show that purpose and legitimacy of specification remain a challenge for investigating officers. "*A continual sort of education piece really to investigating officers ... 'Give me the report' ... 'Give me your download'. Well, we can be better than that*" [PP5]. The request forms need to be informed by intelligence and investigative gaps. "*I don't want police officers to worry about digital forensics. I want them to worry about their interviews and their investigative gaps. What are the intelligence- and investigative gaps?*"[PP5].

The process of iterative redrafting may be avoided or sped up by the investigating officer and digital forensics team working together and agreeing on the investigation request. Guidelines and tools for purpose specification, the (UK) National Decision Model, PACE 1984 and the Section 49 RIPA notice can help to improve quality or achieve the required quality of request forms. In deciding on purpose limitation, it is important to take into account risk, according to the national decision model of policing. This allows police officers to justify decisions on the scope of a digital forensics examination request based on risk assessment. In relation to digital forensic investigation, legislation has not been able to keep up with advances in technology; for example, legislators seem to lack an understanding of potential problems associated with examiners accessing device users' account on the Internet.

Principle 3: Collection Limitation: At the triage stage (before detailed digital forensics examination), data minimisation involves the examination of three devices at most. Limitation of data collection is constrained by purpose specification: only data can be collected that are relevant to the purpose specification. Resources of time and cost are practical considerations. Given limited resources available and an increasing volume of digital forensics jobs to process, priorities need to be set regarding what data to collect for each job and/or how urgent the data need to be collected, given the priorities of other jobs. To ensure oversight over data collection, digital forensics departments use internal oversight (within the digital forensics unit) and external oversight (e.g. the legal service). If additional evidence is collected that is not necessary according to the purpose specification, there is a risk of having to act on this additional evidence even if it is not relevant to the case at hand. This may then require more work and add further to the digital forensics department's workload. This risk provides another justification for constraining data collection by the scope of the purpose specification. "*Each piece of evidence that is uncovered may reveal a risk that will need to be dealt with*" [PP7]. It is important to specify the time span (start date and end date) and then collect evidence (for example on a mobile phone) according to the time span. If the time span is too extensive, time will be spent collecting irrelevant records. If the time span is too narrow then important evidence may not be included and the evidence will be incomplete. The information that is extracted will be specific, as much as possible, to the digital forensics examination request. However, specificity is not always possible. For example, when text messages are extracted it may not be feasible to separate different messages.

Principle 4: Data Minimisation: Again, data minimisation is guided by the scope of the purpose specification. Data minimisation is important to speed up the digital forensics examination process, as fewer data examined result in less examination time. "*Even if you wanted to analyse the whole captured image it would take too much time, given the storage volumes on modern devices*" [PP1]. The volume of data examined depends on the seriousness of the offence. "*Normally all the evidence will be examined and the examination will not stop early. However, if only limited time is available to complete the examination then authorisation may be given to stop once a particular volume of evidence has been found and examined, but still the remaining data will be sampled to establish if there is more serious*

evidence" [PP4].

If there is evidence of obfuscation (e.g. data stored in one or more hidden folders ['vaults'] on a device), then the investigation will be prioritised and more data will be examined to ensure no evidence is missed. New technology does not always enable a digital forensics investigator to get a full forensic image from which to select data; therefore, the data set that is examined may be incomplete. Regarding expertise, in order to achieve data minimisation, a specialist or more experienced colleague may work with the digital forensics examiner.

Principle 5: Use, Retention and Disclosure Limitation: It can be a challenge for digital forensics investigations to access data in cloud storage. For example, the user may log in and empty the account after the police have left their home and if it is hosted outside the country's jurisdiction, they will lose the data. Data retention is constrained by digital forensics storage capacity limitations. Therefore, "*Data from a 'negative' device (without useful evidence) is destroyed on job completion*" [PP4]. In addition, there are legal requirements for retention. Moreover, (ISO) industry standards put requirements on retention. This is especially important, as digital forensics lab accreditation may require compliance with relevant standards.

A record needs to be made of what the examination has found; this is disclosable to the defence. Again, this should be guided by the scope of the purpose specification. "*[This way,] the examination can be justified in court as appropriate, proportionate and ethical. There is always a risk that the examination might miss [uncovering] some criminality, but this way a justification can be given for what was done*" [PP7]. The final full digital forensics report including digital forensics evidence is disclosable to the defence.

Principle 6: Accuracy and Quality: Various measures are taken to ensure the accuracy and quality of the evidence, including the following. The examination relies on the functionality that the forensic software provides (a.k.a. 'techniques'). "*Despite differences in techniques, the same process is followed in the application of each technique; in the examination process, the work is double verified, especially when new techniques are used*" [PP2]. Digital forensics examination work is also peer-reviewed for accuracy and quality within the digital forensics unit. For example, verification is done by using multiple digital forensics tools on the same evidence. Quality control is applied to the examination process and the data throughout the process. Competency training, evaluation and review are important and conducted to achieve accuracy and quality of digital forensics investigators' work.

The accuracy and quality of the data, and the examination process are important as they form the basis of the legal process and the outcome of this process. This also extends to the accuracy of digital forensics expert witness statements. In addition, the agreed time span between digital forensics examination team and enquiry officer is crucial. "*If the requested timescale is too short then the request will be rejected. This is to avoid compromising the quality of the examination*" [PP4].

Principle 7: Openness, Transparency and Notice: In order to achieve transparency, records are made of the examination process and justification of decision-making during the process. "*The examinations are done as completely and thoroughly as possible, so anything can be replicated; there is nothing to hide in the process; therefore, the examiner has no objection to the defence agents scrutinising the work*" [PP4]. Giving expert evidence in court can assure transparency. However, there is a limit to transparency: confidential digital forensics techniques that would aid criminals are generally not disclosed.

Principle 8: Individual Participation and Access: Team leaders allocate digital forensics examiners to digital forensics examination jobs. Each examiner on a job has a corroborator; only these two work on the job. Other team members can support the digital forensics examination at the request of the digital forensics examiner and corroborator. "*Any concerns raised would either be by the examiner or the corroborating examiner who would validate the examination*" [PP2]. The digital forensics examiner takes advice from the investigating officer about what to include in the digital forensics report. The digital forensics examiner may request not to proceed with the case if insufficient digital evidence is found.

Principle 9: Accountability: Ultimately, accountability for digital forensics work lies with the digital forensics line manager, but decision-making is done by a senior investigating officer, and the actual investigation is done by the forensic officer in charge of the case. "*Individual technicians (digital forensic investigators) are responsible for the evidence or exhibit throughout the process from the time they received it; they manage their own exhibits*" [PP1]. Accountability for digital forensics examination applies within the scope of the examination request. "*Examiners have to investigate within the scope ['the parameters'] of the enquiry team's request and only report evidence that is within the scope; otherwise, they may be open to questioning in court*" [PP3]. ISO accreditation will contribute to the accuracy and quality of digital

forensic examinations, with an audit trail. At least one of the units was ISO 17025-accredited and others were working towards accreditation. Although accreditation was seen as desirable, the question remains whether ISO accreditation that is not specific for digital forensics is the most appropriate type of certification.

Principle 10: Information Security Controls: The application of information security controls was maintained by ensuring good security practice by digital forensics examiners, ISO accreditation to meet security requirements, complying with legal security requirements and physically secure storage. Security is now part of the process of assessing the quality of the digital forensics unit. Bigger labs have a separate digital forensics lab security team. "*For security, the data are not online; they are on servers that are not on the Internet*" [PP6].

Principle 11: Compliance: Labs applied different methods to achieve compliance, including a checklist, work flow built into case management system, industry standard accreditation and support by the quality team. Although there had been attempts at standardisation in the past, there is currently a lack of standardisation of digital forensics examination process across police forces. "*It's been attempted and never seems to land*" [PP5].

PET use by Citizens

In the experience of the interviewees, PET use had increased in recent years, but this was not quantified. Two explanations for this were advanced. First, 'PET by default': PET availability on devices through pre-installation, so users do not have to install PETs. Second, citizens are more aware of (the availability of) PETs.

An advantage of the use of citizens' PET use was that better self-protection by PETs would lead to fewer cybercrimes, therefore fewer cases to be investigated and consequently a reduced demand on digital forensics services. A disadvantage of citizens' PET use was a hindering digital forensics' access to evidence on devices to be investigated. There were different approaches to access PET-protect evidence on devices, with digital forensics tools. Proportionality was a consideration in attempting to 'break' PETs to get access: a balance had to be struck between the effort required to get access and the potential value of the evidence that might be uncovered with access, given the seriousness of the offence. Password-protected access to evidence in 'the cloud' posed a further challenge, separate from access to evidence on physical devices. Moreover, access to devices was constantly changing because of the 'PETs arms race': digital forensics tools would be developed to circumvent PETs, but then new PETs would be developed that were not yet 'breakable' by the available forensics tools. Finally, different PETs would pose different levels of challenge, for example PETs that restricted access through a password in contrast with PETs did not (for example, information hiding).

"*It is a criminal offence not to give a password in cases where this is required by law with 3-month jail sentence, but for example a possible 10-year sentence if they give their password and crime is established from the evidence on the device. Many suspects of child sex abuse material refuse to give their password. They may weigh up (a) their potential sentence under Section 49 for not giving their password against (b) their potential section for their child sex abuse material crime and decide that (a) is more favourable. Otherwise, they may claim that they have forgotten their password; in that case, Section 49 does not apply. However, it is highly unlikely that they have forgotten their password, because it gives them access to a vast collection of material that they have collected*" [PP6].

Discussion of Findings

In response to RQ1, our results show that privacy principles are taken into consideration in digital forensics work, but that there are challenges in doing this For example a lack of basic training in digital forensics by police officers leads to iterative redrafting of digital forensics examination requests with consequent delays. Automation can help with increasing the timeliness of digital forensics investigations, but requires additional resources in a context of a lack of investment "*in research on automation techniques for the retrieval and analysis of large volumes of digital evidence*" [House of Lords, 2019, p. 5].

In response to RQ2, our findings demonstrate that citizens' increasing use of PETs as well cloud storage is hindering digital forensics investigation. As a result, the additional effort required poses an additional resource allocation problem: balancing the effort required to get access needs against the potential value of the evidence if uncovered successfully as well as the increasing volume of cases.

5. Implications for Practice

Timeliness of digital forensics investigation: Consider basic training to improve communication between investigating officers and digital forensics teams, and reduce the need for redrafting examination requests, thereby increasing the speed and quality of investigation.

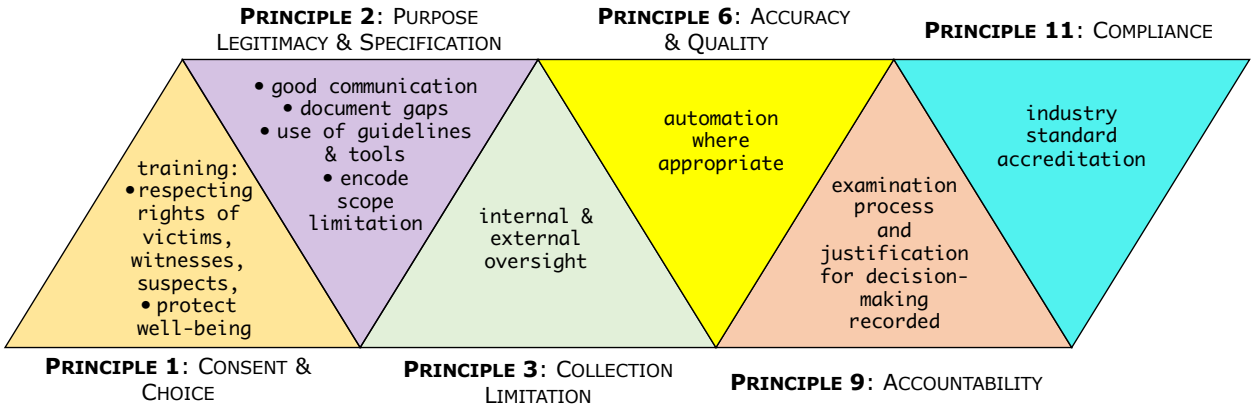

Figure 2. Final Recommendations

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

Privacy Principles: Figure 2 summarises the final recommendations, as follows:

Principle 1: Consent and Choice: Ensure that training covers: (a) respecting human rights of victims and witnesses, but also suspects, and (b) protecting people's well-being.

Principle 2: Purpose Legitimacy and Specification: Ensure good communication between investigating officer and digital forensics team on each case. Ensure intelligence- and investigative gaps are appropriately documented to inform targeted purpose legitimacy and specification for writing a digital forensics request. Use appropriate guidelines and tools to inform purpose legitimacy and specification. In writing a digital forensics request consider the need for scope limitation.

Principle 3: Collection Limitation: Police forces will have a system in place for internal, as well as external, oversight of digital forensics examination.

Principle 6: Accuracy and Quality: Consider using automation where appropriate for accurate consistency and speed.

Principle 9: Accountability: The examination process and justification for decision-making need to be recorded. Consider industry-standard accreditation to ensure an appropriate audit trail.

Principle 11: Compliance: Consider industry standard accreditation for compliance. Standardisation of digital forensics examination process across police forces could provide equity across the country, also in terms of the legal process that uses digital forensics evidence and the outcomes of this process.

6. Conclusion

In this study, we reported on interviews and analysis of privacy as a consideration in police digital forensics investigations. We identified specific uses of privacy-related principles that ought to apply in digital forensics investigations, and issues for digital forensics investigation from citizens' use of PETs. We concluded with potential implications for practice.

In terms of future work, we need to investigate how best to reconcile the security requirements of society at large with the right to privacy of individual citizens. We would also like to analyse stakeholders' perceptions of the privacy-related aspects of digital forensics investigations.

Acknowledgements:

We gratefully acknowledge funding from REPHRAIN for the SelfProtect project and research participation by the digital forensics professionals. This work is supported by REPHRAIN: National Research centre on Privacy, Harm Reduction and Adversarial Influence online (EPSRC Grant: EP/V011189/1).

References

[American Institute of Certified Public Accountants, 2010] American Institute of Certified Public Accountants (2010). GAPP. Generally Accepted Privacy Principles https://linfordco.com/blog/the-10-generally-accepted-privacy-principles/.

[Armstrong and Norris, 2020] Armstrong, G. and Norris, C. (2020). *The maximum surveillance society: The rise of CCTV*. Routledge.

[Bateman, 2023] Bateman, R. (2023). Privacy laws by country. https://www.termsfeed.com/blog/privacy-laws-by-country.

[BBC, 2018] BBC (2018). Australia data encryption

laws explained. https://www.bbc.co.uk/news/world-australia-46463029.

[BBC, 2018a] BBC (2018a). Police Scotland cyber kiosks 'could be unlawful'. https://www.bbc.com/news/uk-scotland-46225771 Accessed 23 March 2023.

[BBC, 2018b] BBC (2018b). Should police be allowed to forensically search mobiles? 16 November. Retrieved 31 May 2023 from: https://www.bbc.co.uk/news/uk-scotland-46232572.

[BBC, 2023] BBC (2023). Police officer 'warned' after using database to find a woman. https://www.bbc.co.uk/programmes/p0fbxk4v Accessed 28 March 2023.

[Bott and Renaud, 2018] Bott, G. J. and Renaud, K. (2018). Are 21st-century citizens grieving for their loss of privacy? In *2018 Dewald Roode Workshop on Information Systems Security Research*. IFIP Working Group 8.11/11.13.

[Braun and Clarke, 2006] Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3:77–101.

[Carlo and Ferris, 2019] Carlo, S. and Ferris, G. (2019). Digital strip searches: The police's data investigations of victims. https://bigbrotherwatch.org.uk/wp-content/uploads/2019/07/Digital-Strip-Searches-Final.pdf Accessed 23 March 2023.

[Casey et al., 2011] Casey, E., Fellows, G., Geiger, M., and Stellatos, G. (2011). The growing impact of full disk encryption on digital forensics. *Digital Investigation*, 8(2):129–134.

[Casey and Stellatos, 2008] Casey, E. and Stellatos, G. J. (2008). The impact of full disk encryption on digital forensics. *ACM SIGOPS Operating Systems Review*, 42(3):93–98.

[Casino et al., 2022] Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., and Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access*, 10:25464–25493. https://doi.org/10.1109/ACCESS.2022.3154059.

[Cavoukian, 2006] Cavoukian, A. (2006). Creation of a global privacy standard. Published November http://www.ehcca.com/presentations/privacysymposium1/cavoukian_2b_h5.pdf.

[Centre for Data Ethics and Innovation, 2021] Centre for Data Ethics and Innovation (2021). Privacy enhancing technologies adoption guide. https://cdeiuk.github.io/pets-adoption-guide/ Accessed 23 March 2023.

[Chaker, 2017] Chaker, V. M. (2017). Your spying smartphone: Individual privacy is narrowly strengthened in carpenter v. united states, the us supreme court's most recent fourth amendment ruling. *J. Tech. L. & Pol'y*, 22:1.

[Cohen et al., 2020] Cohen, I. G., Gostin, L. O., and Weitzner, D. J. (2020). Digital smartphone tracking for COVID-19: public health and civil liberties in tension. *Jama*, 323(23):2371–2372.

[College of Policing, 2021] College of Policing (2021). Obtaining data from digital devices – new guidance released. https://www.college.police.uk/article/extraction-material-digital-devices-app Accessed 28 March 2023.

[Conlan et al., 2016a] Conlan, K., Baggili, I., and Breitinger, F. (2016a). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *Digital Investigation*, 18:S66–S75.

[Conlan et al., 2016b] Conlan, K., Baggili, I., and Breitinger, F. (2016b). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *Digital Investigation*, 18:S66–S75. https://doi.org/10.1016/j.diin.2016.04.006.

[Dehghantanha and Franke, 2014] Dehghantanha, A. and Franke, K. (2014). Privacy-respecting digital investigation. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust*, pages 129–138. IEEE.

[Englbrecht and Pernul, 2020] Englbrecht, L. and Pernul, G. (2020). A privacy-aware digital forensics investigation in enterprises. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pages 1–10. https://doi.org/10.1145/3407023.3407064.

[European Convention, 2012] European Convention (2012). Article 8 of the European Convention on human rights. https://fra.europa.eu/en/law-reference/european-convention-human-rights-article-8-0 Accessed 28 March 2023.

[Ferguson et al., 2020] Ferguson, I., Renaud, K., Wilford, S., and Irons, A. (2020). PRECEPT: a framework for ethical digital forensics investigations. *Journal of Intellectual Capital*, 21(2):257–290. https://doi.org/10.1108/JIC-05-2019-0097.

[Ferguson et al., 2018] Ferguson, R. I., Renaud, K., and Irons, A. (2018). Dark clouds on the horizon: the challenge of cloud forensics. In *9th International Conference on Cloud Computing, GRIDs, and Virtualization*, pages 51–58. International Academy, Research, and Industry Association (IARIA).

[Gentry, 2009] Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 169–178.

[Gross, 1967] Gross, H. (1967). The concept of privacy. *NYUL Rev.*, 4:34–54.

[Hart, 1983] Hart, H. L. A. (1983). *Essays in jurisprudence and philosophy*. OUP Oxford. https://doi.org/10.1093/acprof:oso/9780198253884.003.0002.

[HMICFRS, 2022] HMICFRS (2022). An inspection into how well the police and other agencies use digital forensics in their investigations. His Majesty's Inspectorate of Constabulary and Fire & Rescue Service https://www.justiceinspectorates.gov.uk/hmicfrs/publication-html/how-well-the-police-and-other-agencies-use-digital-forensics-in-their-investigations/.

[House of Lords, 2019] House of Lords (2019). Forensic science and the criminal justice system: a blueprint for change. https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/333/33310.htm Accessed 23 March 2023.

[Irons and Lallie, 2014] Irons, A. and Lallie, H. S. (2014). Digital forensics to intelligent forensics. *Future Internet*, 6(3):584–596.

[ISO, 2011] ISO (2011). Information technology — security techniques privacy framework. ISO/IEC 29100:2011 Standard. International Organization

for Standardization (ISO): Geneva, Switzerland. https://www.natlawreview.com/article/thinking-beyond-law-what-iso-29100-privacy-framework.

[Königs, 2022] Königs, P. (2022). Government surveillance, privacy, and legitimacy. *Philosophy & Technology*, 35(1):8.

[Landesberg et al., 1998] Landesberg, M. K., Levin, T. M., Curtin, C. G., and Lev, O. (1998). Privacy online: A report to congress. Washington, DC.

[McCahill and Norris, 2002] McCahill, M. and Norris, C. (2002). "CCTV in London," Report Deliverable of UrbanEye Project . http://www.urbaneye.net/results/results.htm.

[Muir and Walcott, 2021] Muir, R. and Walcott, S. (2021). Unleashing the value of digital forensics. https://www.police-foundation.org.uk/publication/unleashing-the-value-of-digital-forensics/ Accessed 23 March 2023, The Police Foundation.

[OECD, 2010] OECD (2010). Organisation for economic co-operation and development privacy principles. http://oecdprivacy.org/.

[O'Sullivan, 2020] O'Sullivan, K. (2020). Police Scotland to begin 'phased' rollout of controversial cyber kiosks. https://futurescot.com/police-scotland-begin-phased-rollout-controversial-cyber-kiosks/ Accessed 23 March 2023.

[Reed et al., 1998] Reed, M. G., Syverson, P. F., and Goldschlag, D. M. (1998). Anonymous connections and onion routing. *IEEE Journal on Selected areas in Communications*, 16(4):482–494.

[Reedy, 2020] Reedy, P. (2020). Interpol review of digital evidence 2016-2019. *Forensic Science International: Synergy*, 2:489–520.

[Renaud et al., 2016] Renaud, K., Flowerday, S., English, R., and Volkamer, M. (2016). Why don't UK citizens protest against privacy-invading dragnet surveillance? *Information & Computer Security*, 24(4):400–415. https://doi.org/10.1108/ICS-06-2015-0024.

[Seyyar and Geradts, 2020] Seyyar, M. B. and Geradts, Z. J. (2020). Privacy impact assessment in large-scale digital forensic investigations. *Forensic Science International: Digital Investigation*, 33:200906. https://doi.org/10.1016/j.fsidi.2020.200906.

[The Police Foundation, 2022] The Police Foundation (2022). A new mode of protection redesigning policing and public safety for the 21st century. https://www.policingreview.org.uk Accessed 23 March 2023.

[United Nations, 1948] United Nations (1948). Universal declaration of human rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights Accessed 1 June 2023.

[Van Der Schyff et al., 2023] Van Der Schyff, K., Foster, G., Renaud, K., and Flowerday, S. (2023). Online privacy fatigue: a scoping review and research agenda. *Future Internet*, 15(5):164.

[Weston, 2018] Weston, P. (2018). How police can download the private contents of your phone in minutes without a warrant and with 'no limit on the volume of data'. https://www.dailymail.co.uk/sciencetech/article-5558511/Police-download-phones-data-minutes-NO-warrant.html Accessed 23 March 2023.

[Wu and Radke, 2011] Wu, Z. and Radke, R. J. (2011). Real-time airport security checkpoint surveillance using a camera network. In *CVPR 2011 WORKSHOPS*, pages 25–32. IEEE.

[Ziller and Helbling, 2021] Ziller, C. and Helbling, M. (2021). Public support for state surveillance. *European Journal of Political Research*, 60(4):994–1006. https://doi.org/10.1111/1475-6765.12424Citations:1.

Appendix A: Interview Questions

Part 1: the use of data collection techniques and investigation techniques

small First, I would like to ask you about the potential use of a number of privacy-related principles that may be applied in digital forensic investigation.

1.1. For each principle, in your experience, is it applied? **1.2.** If so, how? **1.3.** If not, why not? For example, it may conflict with specific requirements of the investigation. **P1**: Consent & Choice; **P2**: Purpose Legitimacy and Specification; **P3**: Collection Limitation; **P4**: Data Minimization; **P5**: Use, Retention and Disclosure Limitation; **P6**: Accuracy and Quality; **P7**: Openness, Transparency & Notice; **P8**: Individual Participation and Access; **P9**: Accountability; **P10**: Information Security Controls; **P11**: Compliance.

Part 2: citizens' use of PETs in relation to investigation

Second, I would like to ask you about citizens' use of privacy-enhancing technologies (PETs) in relation to data collection and investigation.

2.1. For each category of PET, does citizens' use of privacy-enhancing technologies (PETs) hinder data collection and investigation? **2.2.** If so, how? **2.3.** If not, why not? For example, it may conflict with specific requirements of the investigation.

Table 2. A Sample of Country Privacy Laws [Bateman, 2023]

COUNTRY	LAW
Argentina	Personal Data Protection Act
Australia	Privacy Act 1988
Brazil	Brazilian General Data Protection Law
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)
European Union	General Data Protection Regulation (GDPR)
Japan	Act on the Protection of Personal Information
Mexico	Federal Law on the Protection of Personal Data held by Private Parties
New Zealand	Privacy Act 1993
Nigeria	The Nigerian Data Protection Regulation 2019
South Africa	Protection of Personal Information Act 4 of 2013
Sweden	Protective Security Act
USA	California Consumer Privacy Act (CCPA); Colorado Privacy act; Colorado's CPA