PRECEPT: A FRAMEWORK FOR ETHICAL DIGITAL FORENSICS INVESTIGATIONS

Journal:	*Journal of Intellectual Capital*
Manuscript ID	JIC-05-2019-0097.R2
Manuscript Type:	Research Paper
Keywords:	Digital Forensics Investigation, Ethics, Privacy, Intellectual capital
Abstract:	

MANUSCRIPT DETAILS

: PRECEPT: A FRAMEWORK FOR ETHICAL DIGITAL FORENSICS INVESTIGATIONS

:enabled crimes are on the increase, and law enforcement has had to expand many of their detecting activities into the digital domain. As such, the field of digital forensics has become far more sophisticated over the years and is now able to uncover even more evidence that can be used to support prosecution of cyber criminals in a court of law. Governments, too, have embraced the ability to track suspicious individuals in the online world. Forensics investigators are driven to gather data exhaustively, being under pressure to provide law enforcement with sufficient evidence to secure a conviction.

Yet, there are concerns about the ethics and justice of untrammeled investigations on a number of levels. On an organizational level, unconstrained investigations could interfere with, and damage, the organizationâ€™s right to control the disclosure of their intellectual capital. On an individual level, those being investigated could easily have their legal privacy rights violated by forensics investigations. On a societal level, there might be a sense of injustice at the perceived inequality of current practice in this domain.

This paper argues the need for a practical, ethically-grounded approach to digital forensic investigations, one that acknowledges and respects the privacy rights of individuals and the intellectual capital disclosure rights of organisations, as well as acknowledging the needs of law enforcement. We derive a set of ethical guidelines, then map these onto a forensics investigation framework. We subjected the framework to expert review in two stages, refining the framework after each stage. We conclude by proposing the refined ethically-grounded digital forensics investigation framework. Our treatise is primarily UK based, but the concepts presented here have international relevance and applicability.this paper, the lens of justice theory is used to explore the tension that exists between the needs of digital forensic investigations into cybercrimes on the one hand, and, on the other, individualsâ€™ rights to privacy and organizationsâ€™ rights to control intellectual capital disclosure.investigation revealed a potential inequality between the practices of digital forensics investigators and the rights of other stakeholders. That being so, the need for a more ethically-informed approach to digital forensics investigations, as a remedy, is highlighted, and a framework proposed to provide this.proposed ethically-informed framework for guiding digital forensics investigations suggest a way of re-establishing the equality of the stakeholders in this arena, and ensuring that the potential for a sense of injustice is reduced.proposed ethically-informed framework for guiding digital forensics investigations suggest a way of re-establishing the equality of the stakeholders in this arena, and ensuring that the potential for a sense of injustice is reduced.theory is used to highlight the difficulties in squaring the circle between the rights and expectations of all stakeholders in the digital forensics arena. The outcome is the forensics investigation guideline, PRECEpt: Privacy-Respecting EthiCal framEwork, which provides the basis for a re-aligning of the balance between the requirements and expectations of digital forensic investigators on the one hand, and individual and organizational expectations and rights, on the other.

Responses to Editor & Reviewers

JIC-05-2019-0097: PRECEPT: An Ethical Digital Forensics Investigation Framework

Dear Editor and Anonymous Reviewers:

We are very grateful for the time the reviewers spent reviewing the revision of our paper and the effort they have put into making very helpful, constructive and relevant comments. The tables below explain how we addressed each comment in detail.

Editor Comment	**Response**
The paper has moved very close to acceptance, with one reviewer suggesting minor changes and the other one recommending major revisions, but with only one actual major concern - the lack of data to support the contribution. That reviewer actually says the paper is interesting and written well, so I will discount the call for new data, and ask you to satisfy all other concerns in this final round of revisions. I look forward to your revision.	We are pleased that you, and the reviewers, find that we have improved our paper. We have now added an additional expert review with 14 expert forensics investigators, which led to the addition of a new ethical principle and further refinements to the framework itself. We explain how we have addressed the reviewers' comments below. We would note that it has been difficult to address all these requirements in the light of the fact that the paper is already on the long side. If you, the editor, want us to add more text either to the introduction or conclusion we shall be pleased to do so.

	Reviewer 1	**Response**
R1.1	The paper provides new and significant information that justify publication. However, the originality of the paper along with its contribution should be emphasized more in the introduction and in the conclusions. In both sections, I think it is important to emphasize why and how your study is unique in the field of study. In addition, I think that the introduction should be expanded in order to outline the structure of the paper. I mean, the paper is long and full of different aspects and sections. The introduction should be expanded to let the reader understand how the paper is structured. For example, you should mention and emphasize more the analysis conducted in section 7. In particular, as stated in the individual sections of the comments in this review, I think it is necessary: - to put more emphasis on the contribution both in the introduction and in the conclusions; - to expand the introduction to explain how the paper is structured; - to expand the conclusions to explain how the paper was structured and how the different sections contributed to providing useful and relevant insights.	We have now added the following to the introduction: *In the digital forensics domain, it is appropriate for us to ensure that there is no injustice in the way digital forensics investigations are carried out, because the day might come when any one of us could become the subject of such an investigation. Moreover, as Irons and Konstadopoulou (2007) argue, the field of digital forensics requires a codified body of principles as well as standards for ethics and practice if it is to be considered a profession. Dehghantanha and Franke (2014) make a strong case for the need of a framework for privacy-respecting digital investigations, but do not propose such a framework themselves. Aminnezhad et al (2012) write a treatise on the tensions between digital forensics investigators and privacy preserving technologies, but they, too, do not propose a framework to resolve the tensions. Antoniou et al. (2006) and Croft and Olivier (2010) do propose privacy-preserving frameworks, but their measures are technological, and not ethically-grounded, which is what we are proposing, as advocated by Irons and Konstadopoulou (2007). Why specifically a framework? Because a framework provides a helpful structure to guide and inform investigations, a way for investigators to chart their progress. It serves to highlight pertinent ethical considerations as investigators carry out their investigation.* *Figure 1 depicts this paper's argument and layout. We commence by highlighting the current state of play in the digital forensics investigation domain (Section 2). In particular, we present both sides of an apparent impasse: individual and organizational rights on the one hand, and*

	- to emphasize more the analyses conducted in section 7. The results must be tied with the literature. This linkage should be emphasized in the introduction.	*forensics investigation capabilities on the other. We argue for the need for a sweet spot, which maximizes utility for stakeholders on either side of the metaphorical tug-of-war. Section 2 provides a road map outlining the rest of the paper, which presents the perspectives of digital forensics investigations (Section 3), and those of individuals and organizations (Section 4). Principle lists of basic privacy, intellectual capital, investigation guidelines and ethical principles are derived from the research literature and enumerated for subsequent use in deriving the framework.* *Section 5 then compiles a set of ethical principles which can guide and inform digital forensics investigations. Section 6 discusses the tensions between the two somewhat opposing perspectives. Section 7 brings all the new insights together to propose a privacy-respecting framework that balances these tensions, in effect driving us towards the "sweet spot" we proposed in Section 2. The framework incorporates eight forensic investigation stages, which are mapped onto the listed ethical principles as well as the challenges constituted by "dark clouds" caused by the emergence of modern privacy-protecting technologies.* *Section 7 details our expert evaluation of the framework, in two phases, and presents the final PRECEPT framework. Section 8 concludes.* *The contributions of this paper are three-fold: First, we apply justice theory to the field of digital forensics investigations. Second, propose a set of eleven ethical principles to inform digital forensics investigations. Third, we provide an ethically informed privacy respecting digital investigation framework that was subjected to expert review as a remedy to bring a sense of equality and justice back into this domain.* We also moved the old Fig 2 (now Fig 1), which depicts the paper's argumentation, into the introduction, to give the reader an overview of the paper and help them to traverse the different sections. We have also extended both Figs 1 and 3 to include the expert evaluation of the framework. Finally, we extended the conclusion to summarize the contributions of the paper more comprehensively.
R1.2	I just suggest discussing more the role of recent studies in the introduction. What is the contribution of the recent literature? Please emphasize it in the introduction.	We have included the following paragraph in the introduction to address this: "*In the digital forensics context, it is appropriate for us to ensure that there is no injustice in the way digital forensics investigations are carried out, because the day might come when any one of us could become the subject of such an investigation. Moreover, as Irons and Konstadopoulou (2007) argue, the field of digital forensics requires a codified body of principles as well as standards for ethics and practice if it is to be considered a profession. Dehghantanha and Franke (2014) make a strong case for the need for a framework for privacy-respecting digital investigations, but do not propose such a framework themselves. Aminnezhad et al (2012) write a treatise on the tensions between digital forensics investigators and privacy preserving technologies, but they, too, do not propose a framework for attempting to resolve the tensions. Antoniou et al. (2006) and Croft and Olivier (2010) do propose frameworks to preserve privacy, but their measures are technological, and not ethics-based, which is what we are proposing* as advocated by Irons and *Konstadopoulou (2007)*"

R1.3	I suggest mentioning the survey (Appendix A) in the abstract.	We thought this was a good idea but we have been advised not to include specific section references in the abstract.
R1.4	Implications for research, practice and/or society: The last section is too small. I suggest expanding the conclusion by providing theoretical and practical implications. Moreover, as anticipated, the paper is long, with many sections. The last section should draw conclusions by briefly illustrating the contribution of the various sections.	We added the following paragraph to the conclusion: "*We drew from the literature on privacy, intellectual capital, investigative guidelines, ethics, anti-forensics and forensics investigation stages to derive at an ethically-informed framework to guide digital forensics investigations. We subjected the derived framework to expert review and refined it accordingly. In proposing PRECEPT, we follow the recommendations of a number of researchers, who highlight the need for a privacy-protecting framework which balances the needs of investigators with the rights of individuals and organizations*."

	Reviewer 2	**Response**
R2.1	This paper raises an important question of ethics in digital investigation process. The paper is well written and the overall idea is nicely articulated.	Thanks!
R2.2	Overall, the authors have cited many relevant papers. There are other papers that could be worked into the discussion like: https://www.sciencedirect.com/science/article/pii/S1742287606000661 https://heinonline.org/HOL/Page?handle=hein.journals/digiteeslr4&div=11&g_sent=1&casa_token=cZ8mFaGPht4AAAAA:HbFapWnqaMvZHHUGrmOZ4zok9w12GHO3AGpeKVxholVcN1arJzSHERTUW5dzk2Bjl4pL8s90Xb4&collection=journals	Thanks for suggesting these papers. We have now included their insights in our paper.
R2.3	This paper identifies the implication of this research on society as whole. With the rise in cases involving computers and other digital devices, it is very much necessary for a digital investigator to understand the ethics that will further help them in conducting the investigation by protecting the rights of the people. The paper has also proposed various ideas that is not only valid theoretically; rather they are also valid practically.	Thanks!

PRECEPT: A Framework for Ethical Digital Forensics Investigations

Abstract

Purpose: Cyber-enabled crimes are on the increase, and law enforcement has had to expand many of their detecting activities into the digital domain. As such, the field of digital forensics has become far more sophisticated over the years and is now able to uncover even more evidence that can be used to support prosecution of cyber criminals in a court of law. Governments, too, have embraced the ability to track suspicious individuals in the online world. Forensics investigators are driven to gather data exhaustively, being under pressure to provide law enforcement with sufficient evidence to secure a conviction.

Yet, there are concerns about the ethics and justice of untrammeled investigations on a number of levels. On an organizational level, unconstrained investigations could interfere with, and damage, the organization's right to control the disclosure of their intellectual capital. On an individual level, those being investigated could easily have their legal privacy rights violated by forensics investigations. On a societal level, there might be a sense of injustice at the perceived inequality of current practice in this domain.

This paper argues the need for a practical, ethically-grounded approach to digital forensic investigations, one that acknowledges and respects the privacy rights of individuals and the intellectual capital disclosure rights of organisations, as well as acknowledging the needs of law enforcement. We derive a set of ethical guidelines, then map these onto a forensics investigation framework. We subjected the framework to expert review in two stages, refining the framework after each stage. We conclude by proposing the refined ethically-grounded digital forensics investigation framework. Our treatise is primarily UK based, but the concepts presented here have international relevance and applicability.

Design methodology: In this paper, the lens of justice theory is used to explore the tension that exists between the needs of digital forensic investigations into cybercrimes on the one hand, and, on the other, individuals' rights to privacy and organizations' rights to control intellectual capital disclosure.

Findings: The investigation revealed a potential inequality between the practices of digital forensics investigators and the rights of other stakeholders. That being so, the need for a more ethically-informed approach to digital forensics investigations, as a remedy, is highlighted, and a framework proposed to provide this.

Practical Implications: Our proposed ethically-informed framework for guiding digital forensics investigations suggest a way of re-establishing the equality of the stakeholders in this arena, and ensuring that the potential for a sense of injustice is reduced.

Originality/value: Justice theory is used to highlight the difficulties in *squaring the circle* between the rights and expectations of all stakeholders in the digital forensics arena. The outcome is the forensics investigation guideline, PRECEpt: *Privacy-Respecting EthiCal framEwork*, which provides the basis for a re-aligning of the balance between the requirements and expectations of digital forensic investigators on the one hand, and individual and organizational expectations and rights, on the other.

Keywords: Forensics Investigations, Ethics, Privacy, Intellectual Capital.

Paper type: Conceptual

1. Introduction

Rawls' (1991) Theory of Justice is built on two core principles: *liberty* and *equality*. Working in tandem, they designate that society ought be structured so that the greatest possible amount of liberty is provided to its members, the proviso being that the liberty of any one individual not be permitted to infringe upon that of any other. Moreover, any inequalities that *do* exist ought only to be permitted if equality would leave people worse off. Deutsch (1986) introduces the concept of *distributive justice* as a way of envisioning whether these principles are being achieved in any society. Deutsch reports on a number of experimental studies he carried out to investigate the sense of *injustice* in society, and recounts a range of insights gained from these. Of particular relevance to our context is that those who are disadvantaged by inequality are more sensitive to the injustice thereof than those who are advantaged by such inequalities. Adams (1965) argues that an experience of injustice should not be an accepted fact of life. Kant's *categorical imperative* (O'Neill, 1993) requires everyone to act only in such a way that they would consider fair if applied universally across society. Deutsch (1986) argues that sensitivity to injustice across society can be increased by acknowledgement of inequalities and by providing viable remedies.

The focus in this paper is on digital forensics investigations, and their potential for being perceived as unjust. George Orwell's infamous Big Brother (Orwell, 1949) has, for some, materialized some six decades after the book was published (Sorell and Draper, 2012) due to ubiquitous digital surveillance and rapacious digital investigations. David Patterson, then ACM President (Patterson, 2005) expressed these concerns trenchantly: "*We must protect the security and privacy of computer and communication users from criminals and terrorists while preventing the Orwellian vision of Big Brother. Computer and communication in the 21st century should be as safe as 20th century banking*" (p. 16).

In the digital forensics domain, it is appropriate for us to ensure that there is no injustice in the way digital forensics investigations are carried out, because the day might come when any one of us could become the subject of such an investigation. Moreover, as Irons and Konstadopoulou (2007) argue, the field of digital forensics requires a codified body of principles as well as standards for ethics and practice if it is to be considered a profession. Dehghantanha and Franke (2014) make a strong case for the need of a framework for privacy-respecting digital investigations, but do not propose such a framework themselves. Aminnezhad *et al.* (2012) write a treatise on the tensions between digital forensics investigators and privacy preserving technologies, but they, too, do not propose a framework to resolve the tensions. Antoniou *et al.* (2006) and Croft and Olivier (2010) do propose privacy-preserving frameworks, but the measures they deploy are technological, and not ethically-grounded, which is what we are proposing to do, as advocated by Irons and Konstadopoulou (2007). Why specifically a framework? Because a framework has the ability to structure, guide and inform investigations, providing a way for investigators to chart their progress. Moreover, its very structured nature serves as a convenient harness for highlighting pertinent ethical considerations as investigators work through the stages during their investigations.

Figure 1 depicts this paper's argument and layout. We commence by highlighting the current state of play in the digital forensics investigation domain (Section 2). In particular, we present both sides of an apparent impasse: individual and organizational rights on the one hand, and forensics investigation capabilities on the other. We argue for the need to home in on an elusive "sweet spot", which maximizes utility for stakeholders on both sides of the metaphorical tug-of-war. Section 2 ends with a road map outlining the rest of the paper, which presents the perspectives of digital forensics investigations (Section 3), and those of individuals and organizations (Section 4). Principle lists of basic privacy, intellectual capital, investigation guidelines and ethical principles are derived from the research literature and enumerated for subsequent use in deriving the framework.

Section 5 then compiles a set of ethical principles which can guide and inform digital forensics investigations. Section 6 discusses the tensions between the two somewhat opposing perspectives. Section 7 brings all the new insights together to propose a privacy-respecting framework that balances these tensions, in effect driving us towards the "sweet spot" we propose in Section 2. The framework incorporates eight forensic investigation stages, which are mapped onto the listed ethical principles as well as the challenges constituted by "dark clouds" caused by the emergence of modern privacy-protecting technologies.

Section 7 details our expert evaluation of the framework, in two phases, and presents the final PRECEPT framework. Section 8 concludes.

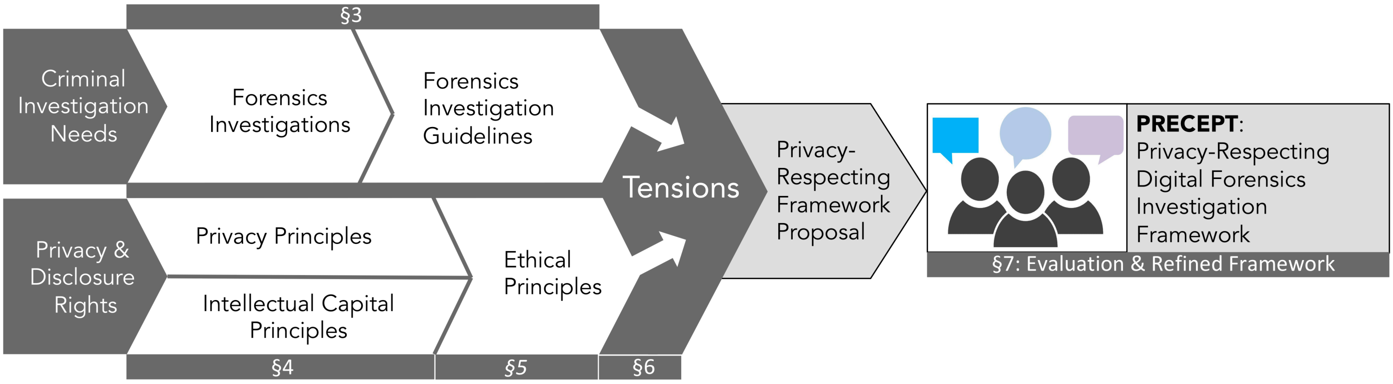
§3
Criminal Investigation Needs
Forensics Investigations
Forensics Investigation Guidelines
Privacy & Disclosure Rights
Privacy Principles
Intellectual Capital Principles
Ethical Principles
Tensions
Privacy-Respecting Framework Proposal
PRECEPT: Privacy-Respecting Digital Forensics Investigation Framework
§7: Evaluation & Refined Framework
§4
§5
§6

Figure 1: The derivation of the ethical framework (Section numbers indicated within the diagram)

The contributions of this paper are three-fold: First, we apply justice theory to the field of digital forensics investigations. Second, propose a set of eleven ethical principles to inform digital forensics investigations. Third, we provide an ethically informed privacy-respecting digital investigation framework that was subjected to expert review as a remedy in terms of introducing a sense of equality and justice back into this domain.

2. Current State of Play

Technology has changed our lives, mostly for the better. Yet there are undeniably those who elect to use computing power for nefarious purposes. When their activities come to light, law enforcement seizes devices for analysis by forensics experts. Forensics investigations in the physical realm have a long and illustrious history (Locard, 1904); digital forensics emerged much later in response to the rising incidence of cyber crime.

Computer forensic evidence has been used since the mid 1990s in the UK, although there was "ad hoc" use of computer evidence in the decade before that (Swarb.co.uk, 2019). The first forensic computing company, AccessData, was established in the late 1980s. In the UK, a fraud case in the Northumbria Police region in 1994 was one of the first to use computer evidence (Turner, 1994). The UK's Association of Chief Police Officers (ACPO) produced their first set of guidelines for dealing with computer evidence in 1996, contributing towards a more structured approach to gathering computer evidence[1]. Rigorous forensics procedures became established, almost organically, and were quickly adopted by forensics investigators (McKemmish, 1999). Universities in the UK started to consider cybercrime in ethics modules in the late 1990s, which then led to the consideration of digital evidence both within education and by crime investigations. This, in turn, led to the development of specialist modules, and programmes in Computer Forensics and Ethical Hacking were established in the late 1990s / early 2000s (Lemos, 2007). Although it would appear that computer forensics has been established for a number of years, it remains a relatively new field, as compared to other kinds of forensics investigations carried out by law enforcement. As recently as 2009, Irons *et al.* debated whether computer forensics was a branch of computer science, a branch of forensic science or a discipline in its own right, and concluded that it is indeed a distinct discipline, meriting independent professional status. This confirms Longhetti's argument made in 1983: "*There is literally no end to the number of disciplines that become 'forensic' by definition. Nor is there an end in sight to the number of present or future specialties that may become forensic. The examples are many*" (p. 3).

Prosecution of cyber crimes has required the enactment of laws, in the USA the Computer Fraud and Abuse Act and in the UK the Computer Misuse Act, for example. Yet in the USA there are concerns that the Computer Fraud and Abuse Act, now three decades old, uses overly vague language, is being interpreted by different prosecutors in different ways, and needs to be reviewed (O'Driscoll, 2018). In the UK, the Computer Misuse Act was enacted in 1990, and reviewed in 2002. Macewan (2008) welcomes the changes,

[1] https://www.digital-detective.net/acpo-good-practice-guide-for-digital-evidence/

arguing that the original act was born prematurely and was too weak to cope with the challenges presented when the Internet arrived in force. Yet Macewan also argues that the updated act has some problems, in particular, that provisions: "*invite controversy, could sometimes prove difficult to interpret or enforce, and may lead to claims of legislative overkill*" (p. 7). These are the signs of a forensics discipline coming into its own, and laying down rigorous principles and practices.

The field of digital forensics has developed established processes and procedures to ensure that the outcomes of such investigations produce evidence that can be used to prosecute miscreants (Casciani, 2019). It is important for such forensics investigations to be carried out as rigorously as any other kind of investigation. Judges in the USA determine the admissibility of digital evidence by using the Daubert test (Adams, 2012), while Ward (2015) reports on a version of this test that has been adopted in England and Wales, called the *Practice Direction*. These tests require the use of a forensics methodology that has been subjected to peer review, and for which the error rate is known. In addition to ensuring that their investigation methodology satisfies the Daubert and similar tests, forensics investigators have to keep up with ongoing technological advances *and* stay ahead of increasingly sophisticated cyber criminals (Pool and Custers, 2017). Law Enforcement has risen to the digital forensics investigation challenge. The UK's College of Policing (2015) states that: "*The Internet is now in most of our homes and while it is a great convenience for us, it also comes with a darker side and these materials and 'how to' investigate guides and videos will help staff to raise their awareness of investigative capability and signpost them to experts who can help further*." The USA's Officer.Com website (2019) states that "*With the proper training and equipment, any law enforcement officer can use the software programs used to extract data from phones in order to strengthen a case*".

This brief summary demonstrates that the field of digital forensics, though relatively young, has earned the right to call itself a discipline, and that law enforcement and educational institutions are developing training to ensure that effective investigations can indeed be carried out in the digital world to support law enforcement. Recently even traditional crimes have been prosecuted with the help of digital forensics to provide evidence of previous online activities, such as Google searches, to demonstrate premeditation (The Investigator, undated).

Concerns related to the way many of these investigations are carried out have been expressed (Big Brother Watch, 2019, Sloan, 2015). Traditional investigations are constrained by law, with well-established codes of practice restricting traditional law enforcement investigations. To many, it seems as if digital investigations are not yet as tightly monitored and constrained, and that individual and organizational rights might be sacrificed in the process (Big Brother Watch, 2018). A recent case in the USA is pertinent here. In the case of Carpenter v. The United States, the FBI had accessed mobile phone connection location data, without a warrant (Oyez, 2018). The Supreme Court ruled, in 2018, that this had breached his privacy rights and stated that future investigations of this kind should undergo judicial overview.

It is interesting to note that the College of Policing website, in discussing their cybercrime courses, do not mention privacy, and their Code of Ethics (2014) does not mention privacy or cyber crime at all. The Officer.Com website (2019) also does not mention privacy in their article. Harrington (2014) argues that digital examiners are not well equipped to manage the ethical dilemmas created by forensics investigations, concluding that: "*the reasons include the lack of industry regulation, a paucity of ethics coverage in training curricula, and that the law applied to this subject matter is not well settled*". This suggests that ethical norms have not yet solidified due to the newness of the field.

Figure 2 depicts the tension between the needs of law enforcement, on the one hand, and privacy and confidentiality rights of individuals and businesses, on the other, as prevalent today as it was in 2005. The arrows at the top and bottom depict the forces pulling in opposite directions. In the interests of societal justice, the situating of the "sweet spot" needs to be seriously considered, and the tensions pulling it in either direction explored. The aim is to ensure a balance that respects the rights of all stakeholders and maximises equality and liberty for all. Here we propose a framework to inform such investigations, in our attempt to start homing in on this "Sweet Spot".

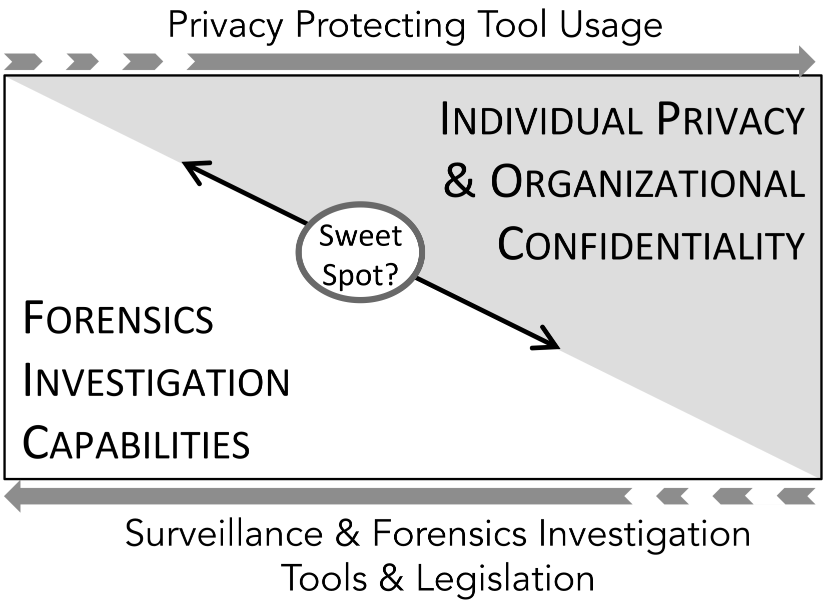
Privacy Protecting Tool Usage
INDIVIDUAL PRIVACY & ORGANIZATIONAL CONFIDENTIALITY
Sweet Spot?
FORENSICS INVESTIGATION CAPABILITIES
Surveillance & Forensics Investigation Tools & Legislation

Figure 2: The Tension between Privacy & Confidentiality Desires and Rights, and Forensics Investigation Needs and Capabilities

Other researchers have also proposed and reviewed forensics investigation frameworks. Agarwal and Kothari (2015) reviewed a number of forensics frameworks, but do not mention privacy considerations. Gupta (2013) proposes automating much of the investigation to maximise privacy. Aminnezhad *et al.* (2012) reviews the privacy challenges of privacy in forensics investigations, concluding that some privacy invasion is unavoidable, and raises the point that privacy decisions are ambiguous by nature, with decisions being made subjectively by an investigator perhaps not matching the expectations of the person being investigated. Their recommendation is that people should deploy privacy-preserving technologies to prevent wholesale privacy invasion. Ieong (2006) proposes a framework that incorporates legal strictures from the USA, but does not mention privacy.

Some researchers have proposed specific privacy-preserving digital forensics investigative frameworks. For example, Nieto *et al.* (2018) propose a framework called PRoFIT, which aims to elicit the cooperation of the citizen into the digital investigation process, respecting the 11 ISO privacy principles at the relevant stage of the investigative process. While this framework achieves its aim of privacy preservation, one can imagine that its applicability will be somewhat limited, given the fact that few criminals will cooperate in an investigation of their devices. Halboob *et al.* (2011, 2015) propose four privacy levels of data that could be uncovered in a forensics investigation, and suggest that courts of law could enforce these to protect the investigatee's privacy during forensics investigations.

In deriving the PRECEPT framework, a justice theory perspective is applied, the first time the tensions have been explored using this lens.

In order to develop the framework for this paper, a "mixed methods" methodology was adopted. This approach was selected in order to draw on existing processes, procedures and frameworks and then to design the proposed framework and undertake an initial test of the framework. The initial data was gathered via a desktop review of existing processes and procedures used for digital forensic investigations in the UK. Particular emphasis was placed on investigating UK legislation, UK procedures (e.g. ACPO) which shape law enforcement practices and the theory, literature and legislation surrounding privacy and the rights of individuals and organisations in the UK.

Figure 3 shows how this investigation was structured, with the notations used throughout the paper indicated within the diagram.

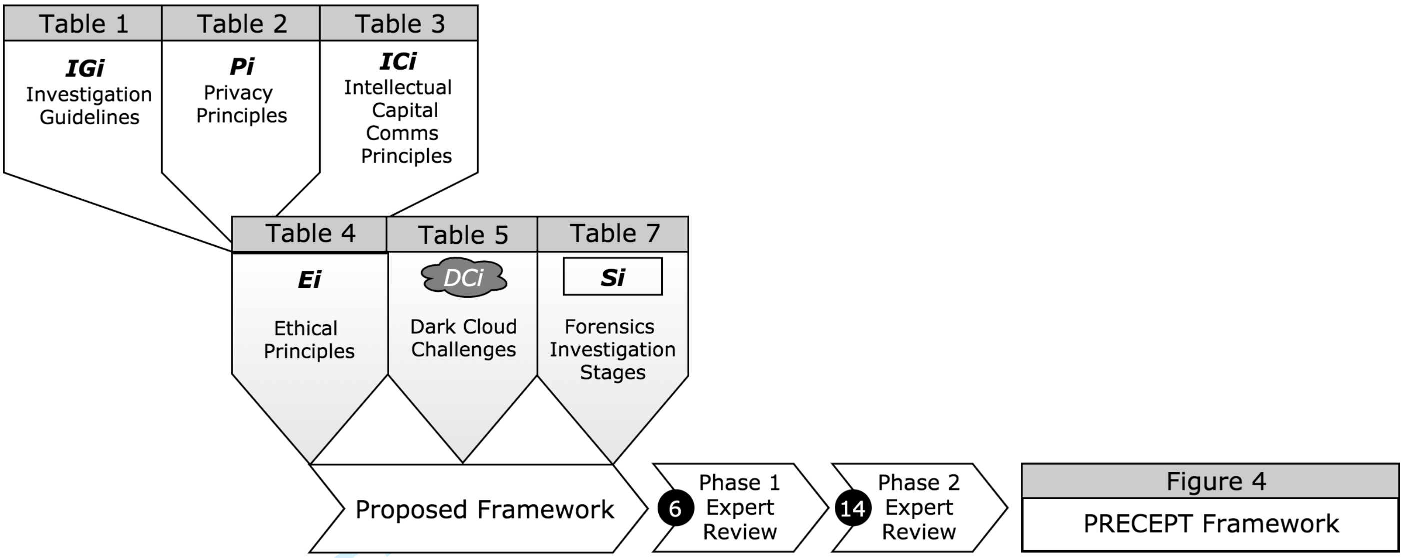

Figure 3: Mapping *Privacy Principles* (*Pi*), *Intellectual Capital Communications Principles* (*ICi*) and *Investigation Guidelines (EGi)* to *Ethical Principles* (*Ei*), and then aligning these with the stages involved in forensics investigations (*Si*) and the challenges introduced by the Dark Clouds (*DCi*), producing the **PRECEPT** framework.

3. Forensics Investigation Perspective

Digital evidence can be used in a range of different types of investigations. For example, digital forensic evidence can be used in organisations to investigate behavioral or disciplinary concerns or internal fraud. Forensics investigations are carried out to uncover evidence of crime, or to detect suspicious behaviors that might lead to a crime or precede a terrorist incident. These are both essential activities, the first being carried out to lead to a successful prosecution, the second to prevent carnage. The forensics investigator systematically analyses data from a suspect's device(s), such as conversations, contacts or evidence of accessing dubious online materials, to gather and accumulate incriminating evidence. The investigation may lead the investigator also to explore other people's devices if there is evidence that they, too, might be of interest or involved in the crime.

Forensics investigations are informed by three guidelines: (1) the Core Investigative Doctrine (CENTREX, 2015), (2) the Criminal Procedure and Investigations Act (CPIA) 1996, which lays out a code of practice for criminal investigations, and (3) the Association of Chief Police Officers, which has published a "good practice guide" for digital evidence (ACPO, 2012). The first two are not specific to cyber crimes.

The digital forensics investigator faces a number of challenges beyond the fact that such doctrines are not specific to their endeavors. Karie *et al.* (2015) present four categories of challenges that forensics investigators face: (1) technical, (2) legal, (3) personnel-related, and (4) operational. Within the focus of this discussion, the first two are worth exploring.

In terms of *technical* challenges, the growing problem for forensics investigators is that it is becoming more and more difficult to gather such evidence from computer systems that are now designed with built-in privacy and security (Langheinrich, 2001). In essence, as systems become resistant to the efforts of hackers, they also resist the forensic investigations. The use of add-on privacy-respecting tools, and their incorporation into operating systems, has become widespread and increasingly effective (Caviglioni *et al.*, 2017). This means that society is reaching a point where everyone can enforce his or her own privacy.

An exception to this may be a reduced expectation of privacy for company-owned equipment used by employees e.g. mobile phones and computers. Employers will often place restrictions on access or on user installation of software so that they can undertake their own investigations should the need arise. In such instances, particularly where the employee may also use the equipment for personal reasons, they would have to accept a much lower expectation of privacy (Margulis, 2003). Privacy concerns do arise however, for example, when employees use their own equipment for work-based activities. In such cases, there are ethical concerns as to which circumstances an employer could demand a restriction on the installation of privacy protection software on an employee's personal phone or laptop. It is quite conceivable therefore, that the death of an employee could render forensic investigations of an organizational data breach, impossible, especially if there is no record of the relevant passwords. The blurring of the distinctions between employee and employer, and the ownership of equipment as well as personal data is increasingly problematic (Brown, 2000). The growth in the use of contractors, workers and self-employed contractors who may use their own equipment to undertake business tasks means that organizations may find that their access is somewhat restricted. These people may not be subject to the restrictions on privacy and use of equipment that an employee would, and therefore permission to access the data on that equipment may be refused.

Systems using privacy-enhancing tools are essentially resistant to forensics investigations: the systems repel all and any incomers. As we write, forensics investigations are stymied by the increasing use of these technologies and are unable to gather sufficient evidence to support prosecution (Ferguson *et al.*, 2018). This paper does not address the technical challenges mentioned by Ferguson *et al.*, only incorporates their influence into our proposed framework.

The *legal* challenges mentioned by Karie *et al.* (2015) that pertain to our investigation include: the laws constraining the activities of investigators, ethical issues, and privacy concerns. These challenges are confirmed by NIST (2015). Some countries do not permit surveillance of their own citizens without judicial overview (Forgang, 2009, Oyez, 2018). Other countries permit surveillance without review (UK Government, 2016). Blum (2006) highlight the trans-jurisdictional and international challenges, which make it difficult for governments to prosecute cyber criminals outside their borders, especially if the criminal resides in a country that does not have an extradition treaty with them. In the UK, where the authors reside, there are a number of guidelines that inform digital forensics investigations. These are helpful in giving us an insight into one specific country's perspectives.

3.1. Investigation Guidelines

This section considers the guidelines provided to inform forensics investigations. To enumerate these, three sources were consulted: (1) the Core Investigative Doctrine (CENTREX, 2015), (2) the Criminal Procedure and Investigations Act (CPIA) 1996, which lays out a code of practice for criminal investigations, and (3) the Association of Chief Police Officers, which has published a "good practice guide" for digital evidence (ACPO, 2012). A set of 10 investigative guidelines were derived, referred to as *IGi*, from these sources, as enumerated in Table 1.

#	**Extracts from sources**
IG1	**Exhaustively investigate:** *"In conducting an investigation, the investigator should pursue all reasonable lines of inquiry, whether these point towards or away from the suspect… For example, where material is held on computer, it is a matter for the investigator to decide which material on the computer it is reasonable to inquire into, and in what manner."* (Ministry of Justice, Section 3.5) On page 63 of (CENTREX, 2015), the investigation phase mindset includes: *Gathering "the maximum amount of material".*
IG2	**Comprehensively record all information:** *"That information which is obtained in the course of a criminal investigation and may be relevant to the investigation is recorded."* (CPIA, Part II)
IG3	**Investigate all relevant related parties:** No mention of investigations only into *relevant* third parties. *"If the officer in charge of an investigation believes that other persons may be in possession of material that may be relevant to the investigation, and if this has not been obtained under paragraph 3.5 above, he should ask the disclosure officer to inform them of the existence of the investigation and to invite them to retain the material in case they receive a request for its disclosure."* (Ministry of Justice, Section 3.6)

IG4	**Sensitive material should be recorded but marked as such:** *"If there is any sensitive unused material the officer should complete a sensitive material schedule (MG6D or similar) and attach it to the prosecution file. In exceptional circumstances, when its existence is so sensitive that it cannot be listed, it should be revealed to the prosecutor separately."* (Ministry of Justice, Section 6.7)
IG5	**Record Intangible information:** *"If material which may be relevant to the investigation consists of information which is not recorded in any form, the officer in charge of an investigation must ensure that it is recorded in a durable or retrievable form."* (Ministry of Justice, Section 4.1) *"An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result."* (p. 6) (Principle 3, ACPO, 2012)
IG6	**Give prosecutor record of gathered information:** *"…the prosecutor … is given a written statement that prescribed activities … that have been carried out."* (CPIA, Part II) The prosecutor must — (a) disclose to the accused any prosecution material … , or (b) give to the accused a written statement that there is no material of a description mentioned in paragraph (a). (CPIA, Part I)
IG7	**Retain all information:** Fourth principle of investigative mindset (CENTREX, 2015): "Recording and Collation". (1) The code may include provision about the form in which information is to be recorded. (2) The code may include provision about the manner in which and the period for which— (a) a record of information is to be retained, and (b) any other material is to be retained; (CPIA, Part II) *"The duty to retain material, where it may be relevant to the investigation, also includes in particular the duty to retain material which may satisfy the test for prosecution disclosure in the Act, such as: information provided by an accused person which indicates an explanation for the offence with which he has been charged; any material casting doubt on the reliability of a confession; any material casting doubt on the reliability of a prosecution witness.* *The duty to retain material falling into these categories does not extend to items which are purely ancillary to such material and possess no independent significance (for example, duplicate copies of records or reports)."* (Ministry of Justice, Sections 5.5 & 5.6).
IG8	**Allow accused to inspect information:** *"the accused is allowed to inspect it [the information] or is given a copy of it."* (CPIA, Part II) *"…that the person who is to allow the accused to inspect information or other material or to give him a copy of it shall decide which of those (inspecting or giving a copy) is appropriate;"* (CPIA, Part II)
IG9	**Investigators must be competent to report on investigation**: *"In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions."* (p. 6) (Principle 2, ACPO, 2012)
IG10	**Information Integrity should be maintained:** *"No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court."* (p. 6) (Principle 1, ACPO, 2012) *"The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to."* (p. 6) (Principle 4, ACPO, 2012)

Table 1: Investigation Guidelines

4. INDIVIDUAL AND ORGANIZATIONAL PERSPECTIVES

The digital investigator's perspectives are discussed in the previous section. Yet the right to *privacy* seems to constitute a fifth challenge, an addition to Karie *et al.* (2015)'s list of forensics investigator challenges. This expectation, and use of privacy-protecting tools, impacts forensics investigations. Moreover, when it comes to organizations being investigated, there is also a need to consider how intellectual capital is potentially impacted by forensics investigations. Here, the other stakeholders are considered: first the individual (Section 4.1) and then the organizational (Section 4.2) perspectives and expectations.

4.1. Individual Privacy Rights

The study and concerns of privacy are multi- and cross-disciplinary and include sociology (Rule, 1974, Winner, 1992), Law, (Warren and Brandeis, 1890), history (Westin, 1967) political science (Bennett, 1996) and philosophy (Schoeman, 1984), and yet we are still never too sure what privacy actually is or what its limits are highlighted by several contributors in Barendt (2001). Many governments are serious enough about such privacy rights to enact privacy-related legislation and to impose punitive fines for organizational failures in this respect (Bischoff, 2018, EU Parliament, 2018). Privacy has been described as the protection of someone's personal space and their right to be left alone (Warren and Brandeis 1890); the control over and safeguarding of personal information (Westin 2003); and an aspect of dignity, autonomy, and ultimately human freedom (Schoeman 1992). These definitions pertain to the boundaries between the self and the others or between private and public, but ultimately fail to provide a universally accepted viewpoint.

The right to, and nature of, privacy continues to be debated and has been included in discussions about fundamental ethical questions such as liberty (Mill, 1869) natural rights (Forester and Morrison, 1995) and core values (Moor, 2006). These discussions often conclude that privacy is chiefly an element of security (Moor, 2006) or a property right, which one can retain or dispose of in much the same way as any other possession (Thomson, 1975). Fairweather (2001 p. 310) however, would refute this view to contend that 'children should be entitled to sexual privacy of a sort that it would not be acceptable to buy or sell.' (p. 310). More recently, some of the earlier examinations of the nature and expectations of privacy are being challenged as social media and ever-increasing covert surveillance affect experiences of privacy (Dienlin and Trepte, 2015).

Even if privacy *is* a right in its own sense, rather than as an add-on to other rights, there are differing opinions as to the extent and scope of that right. As Etzioni suggests, '*giving up some measure of privacy serves the common good*' (Etzioni, 1997 p. 1). This view is echoed by lawmakers and security chiefs the world over (Liberty, 2017, Strohm, 2017, Weinberg, 2015) and would almost certainly be seen as important for forensic investigators looking to access data and following digital footprints around the Internet. The NPCC (2019), responding to criticism from Big Brother Watch about their demands for rape victims to allow full access to their mobile phones, say: "*Police have a duty to pursue all reasonable lines of enquiry in every investigation and to meet the disclosure obligations under the Criminal Procedure and Investigations Act. In this digital age, reasonable lines of enquiry often include the examination of material stored on or accessed by digital devices*".

The media and wider society also promote the view that there should be limits on the amount of privacy anyone can expect in that '*individual rights need to be balanced with social responsibilities*' (Deacon, 1998 p. 6). This communitarian viewpoint creates a strong argument against the idea of a fundamental right to privacy, as it also considers that '*autonomous selves do not exist in isolation, but are shaped by the values and culture of communities*' (King, 2001 p.16). In this context, the authors consider that the right to privacy needs to be (Scott-Hayward *et al.*, 2015) against individual action, so that any expectation of privacy is diminished when issues of safety and security within society take priority over individual needs (Kounadi *et al.*, 2015). To inform development of our framework, our deliberations will be grounded in the ISO/IEC 29100:2011 standard (ISO, 2011), which enumerates 11 privacy principles, referred to in this paper as *Pi*, as listed in Table 2.

P1	Consent & choice	P7	Openness, transparency & 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		

Table 2: Privacy Principles

4.2. Organizational Intellectual Capital Needs

Dumay (2016) defines intellectual capital as "*the sum of everything everybody in a company knows that gives it a competitive edge [...] Intellectual Capital is intellectual material, knowledge, experience, intellectual property, information [...] that can be put to use to create [value].*" [p. 169].

Intellectual capital (IC) makes up a large percentage of a company's market value (Blair and Wallman, 2000). Indeed, Klaila and Hall (2000) carried out case studies to show how newly discovered IC was able to effect drastic improvements to the organizations' balance sheets. Leal *at al.*, (2017) cite (Barney, 1991; Chen *et al.*, 2005) to make the point that intellectual capital is a vital strategic asset, that it is capable of giving organizations a competitive advantage and impacts their financial performance. Inkinen (2015) report that there is a significant relationship between IC and an organization's innovative performance and Obeidat *et al.* (2017) find that IC had a positive impact on organizational performance and knowledge sharing. This is confirmed by many other studies, for example, Maditinos *et al.* (2000); Abeysekera (2006); Edvinsson, and Sullivan (1996). Moreover, Guthrie and Petty (2000) argue that IC is even more important in the 21st century because many large corporations have shifted from manufacturing to offering more technologically-focused services, where IC is somewhat intangible, but still valuable.

Brown *et al.* (2005) explain that intellectual capital has to be protected and managed by utilizing a life-cycle management process. In terms of protecting intellectual capital, Brown *et al.* advise that an information classification scheme be used. They recommend having a set of policies and procedures that align with these classifications to control whether or not intellectual capital elements are disclosed. They also recommend using access control measures to protect any intellectual capital that is stored within IT systems. This leads to our first assertion: *(Assertion 1) IC is valuable***.**

Having established that IC is valuable, the next question is whether organizations need to act to protect and preserve their intellectual capital. Some researchers have indeed highlighted disclosure-related risks to IC. Dumay and Guthrie (2017) argue that involuntary disclosures introduce both opportunities and threats to organizations and that these introduce organizations to new risks. Mouritsen *et al.* (2001) refer to the controlled disclosure of IC as a way of disseminating a "true and fair" account of the firm's activities. Brennan (2001) discovered, in her study of the reports of Irish companies, that the majority of companies disclosed very limited amounts of their IC. It seems that IC tends to be kept confidential. White *et al.* (2007) report that smaller companies demonstrate more reluctance to disclose than larger ones. Sciulli *et al.* (2002) analyzed the IC reporting of Australian councils and found that IC reporting was underdeveloped. They argue that the reasons for such paucity of disclosure are unclear, but need investigation. Indeed, Vanini and Rieg (2019) argue that companies: "*should only engage in voluntary ICD if it really reduces information asymmetries and leads to reduced cost of capital or a better reputation*" (p. 349). Whatever the reasons, it is clear that companies do not happily make all their IC publicly available. This leads to our second assertion: *(Assertion 2) IC disclosure should be controlled.*

Organizations want to control the disclosure of their IC, if indeed they decide to disclose any at all (Dumay, 2016). If such controls fail, is it an issue? Baugh *et al.* (1997) detail the damage that can occur if IC is leaked and companies are not able to control its disclosure. Mohamed *et al.* (2006) also highlight the losses of intellectual capital if the organization does not act to preserve it. Finally, Mitrović and Knețević (2016) considers the risks of financial accounting, and cites uncontrolled disclosure as a specific risk in this space. In more general terms, Laperche (2018) also warns against uncontrolled disclosure, which could harm the organization's competitiveness. This leads to our third assertion: *(Assertion 3) If IC is leaked or disclosure uncontrolled, it could damage the organization.* The *EFFAS Commission On Intellectual Capital* (CIC, 2008) publish a list of intellectual capital specific *effective communication* principles, which will be referred to later in this paper as *ICi (*Table 3*)*. These should be given due consideration when contemplating the ethics of forensics investigations within organizations.

IC1	Clear link to future value creation	IC6	Alignment of interests between company and investors
IC2	Transparency of methodology	IC7	Prevention of information overflow
IC3	Standardization	IC8	Reliability and responsibility
IC4	Consistency over time	IC9	Risk assessment
IC5	Balanced trade-off between disclosure and privacy	IC10	Effective disclosure placement and timing

Table 3: Effective Intellectual Capital Communication Principles

5. Ethical rinciples

The investigative needs of governments and law enforcement were discussed (Section 3), as were the individual rights to privacy and organizational rights to confidentiality (Section 4). The aim, in writing this paper, was to derive a framework to inform *ethical* privacy-protecting forensics investigations, where the balance of power is not skewed in any one direction, where equality is balanced and injustice minimized. As a next step, therefore, a set of ethical principles is derived to inform the development of the framework.

5.1. Generic Ethical Guidelines

In 1992, Anderson *et al*. published a Code of Ethics in Decision Making. Number 1.7 is "*Respect the privacy of others*." The IEEE Code of Ethics[2], on the other hand, does not mention respect for privacy at all. Neither of these is specific to digital forensics. The ACM code of ethics general principles 1.6 however explicitly states that *'computing professional should become conversant in the various definitions and forms of privacy and should understand the rights and responsibilities associated with the collection and use of personal information'*(ACM Committee on Professional Ethics, 2018).

There are three widely used ethical guidelines that inform human-related experiments (American Psychological Association (2016); The Belmont Report (1979); The British Psychological Society). Their guidelines can be combined to arrive at the following five principles (Renaud and Zimmermann, 2018): (1) Respect, (2) Justice, (3) Beneficence, (4) Integrity, and (5) Social Responsibility. These inform experiments, but seem to be equally applicable to the forensics investigator's actions, since it is generally a human whose activities are being investigated. Hence these five principles can function as overarching ethical principles for the purposes of this discussion.

5.2. Forensics Investigations Ethical Guidelines

If the focus is narrowed to ethical concerns related to the forensics process, Saleem *et al.* (2014) make the distinction between "hard" and "soft" privacy. He cites Deng *et al.* (2010) to explain that **hard privacy** means sharing as little data as possible. Soft privacy, on the other hand, implies that the subject of the investigation loses control over their data and have to trust the professionalism of the investigator: that they will keep it **confidential** unless it is specifically required by law to disclose it.

Sloan (2015) argues that there is a need for a code of ethics for digital forensics, but that there isn't a universally accepted one at the moment and Losavio *et al.* (2016) agree. Karia (2010) also highlights the need for digital forensics investigations to be conducted within an ethical framework. Papers mentioning ethics in Digital Forensics were searched for. They fell naturally into three main categories, with respect to their treatment of privacy:

Those referring to the need for (hard) privacy considerations to constrain investigations:

- Van Staden (2013): "*This paper considers the key aspects surrounding privacy protection of third parties during the post mortem data analysis phase of digital forensic investigations.*" (p.19).
- Law *et al.* (2011): "*To enable the protection of data privacy, personal data that are not related to the investigation subject should be excluded during computer forensic examination*" (p.1).

[2] https://www.ieee.org/about/corporate/governance/p7-8.html

- Losavio *et al.* (2015): "*This highlights the twin challenges of forensic accessibility in these highly mobile devices and the intense privacy concerns which may now accompany the profiles of people in ways never before possible.*" (p.45).
- John (2012): "*identify and bookmark privacy concerns, e.g. files with credit card numbers or home addresses;*" (p.2).
- Stahl *et al.* (2010): "*While security is of relevance to safeguard privacy, the powerful security and forensics technology contain the potential to do the opposite. Indeed, in the case of forensics technology, the very point of its application to render data visible that users want to hide*" (p.1824)
- Roux and Falgoust (2012): "*Addressing privacy concerns often involves evaluating specific details of the situation, the agents involved, and the agents' expectations.*" (p.43).
- Nikkel (2014): "*driving the need to explore voluntarily set ethical boundaries to reduce the risk of abuse, and protect the privacy of individuals touched by incident response and forensic investigation activity.* " (p. 5).
- Balogun and Zuva, 2017 citing Rössler, 2005: "*When mechanisms that ensure the confidentiality of data flowing through the systems are not put into place, such data become susceptible to unauthorized access by third parties as well as misuse by authorized parties*" (p.57).
- Srinivasan (2007) proposes ten policies of privacy-respecting forensics investigations.

Those referring to the need for confidentiality (soft privacy): disclosure when mandated:

- Digital Forensics Certification Board (undated): "*Not disclose or reveal any confidential or privileged information obtained during an engagement without proper authorization or otherwise ordered by a court of competent jurisdiction;*" This applies to disclosure, not gathering in the first place.
- ISFCE (2019): "*Reveal any confidential matters or knowledge learned in an examination without an order from a court of competent jurisdiction or with the express permission of the client*"
- GIAC (undated): "*I will protect confidential and proprietary information with which I come into contact.*"
- Karie and Venter, 2015: "*Privacy is very important to any organization or victim. Though, in special cases the investigator may be required to share the data or compromise the client's privacy to get to the truth.*" (p.15).
- Irons and Konstadopoulou, 2001: "*This process should include evidence of exhibiting the highest level of ethical behaviour at all times, and maintaining objectivity and confidentiality during an investigation.*" (p.49).

Those referring neither to confidentiality nor privacy:

- Basset *et al.* (2006): "*Uncover all files: normal, hidden, deleted, encrypted, password-protected*" and "*Access the protected and encrypted files, if legal*" - so no mention of privacy as a constraint.
- Sharevski (2015) reviewed the codes of ethics for 12 organizations ranging from the American Academy of Forensic Science to the SANS Institute and the International Society of Forensic Computer Examiners. He consolidated 10 categories of ethical considerations, none of which refer to the privacy of the person being investigated.
- Other codes of ethics: Forensics Science Regulator (2014), Grobler *et al.*, 2006; Seigfried-Spellar and Rogers, 2017.

5.3. Digital Forensics Ethical Guidelines

It is interesting to note that whereas a number of academic papers refer to the need to respect the privacy of the person being investigated, none of the published digital forensics codes of ethics specifically include this tenet, which means that privacy considerations are probably not informing law enforcement investigations at present. Table 4 thus consolidates all the recommendations into a set of 10 ethical principles, which can serve to guide ethical digital forensics investigations, and maps these to the privacy principles from Table 2, the IC communications principles from Table 3, and the generic ethical principles from Renaud and Zimmermann (2018).

Ethical Principle	Detail	Privacy Principle	IC Comms Principle	Generic Ethical Principle
E1	**Delineate Remit:** Commence by carefully delineating the remit of the investigation (Nikkel, 2014, Srinivasan, 2007).	P2, P3		Respect Social Responsibility
E2	**Respect the privacy of the subject:** The privacy of the subject should be protected by only investigating topics identified as being of interest to the investigation (Law *et al.*, 2011; Dehghantanha and Franke, 2014). In particular, examination scope should be identified *before* the investigation proceeds.	P3	IC5, IC7	Justice Beneficence
E3	**Only investigate other parties if there is evidence of their involvement:** The privacy of third parties should be protected by only investigating them if there is evidence that they have been implicated in the topic of the investigation (Van Staden, 2013).	P3	IC10	Justice Beneficence
E4	**Exclude private information:** During investigation, bookmark private information that is irrelevant to the investigation so that it is not included in any report. Examples are personal credit card numbers, personal passport numbers, and national insurance numbers (John, 2012; Dehghantanha and Franke, 2014).	P4		Respect
E5	**Document all actions:** Document all data that was examined, judged private and irrelevant, and relevant to the investigation (Saleem *et al.*, 2014; Srinivasan, 2007).	P6, P7	IC8	Integrity
E6	**Facilitate audits:** Facilitate post-investigation scrutiny (Gay, 2012).	P9		Integrity
E7	**Report all investigative activities:** When the investigation is concluded, the report should include details of exactly what was examined, who was included in the investigation, which devices were examined (and who they belonged to) (Losavio *et al.*, 2015), how data was classified as relevant (to be reported), confidential (only to be reported if the court so orders), irrelevant (not to be divulged) and how the data was preserved to prevent any alteration (Saleem *et al.*, 2014; Roux and Falgoust, 2012).	P5, P10		Integrity
E8	**Be transparent about the extent of the investigation, and the gathered information:** Subjects, and their counsel, have to be given the right to know what data was processed and how it was processed (Saleem *et al.*, 2014).	P9		Respect Justice
E9	**Investigators should undergo regular training:** Investigators should undergo frequent proficiency training and testing (Saleem *et al.*, 2014).	P11		Social Responsibility
E10	**Information's Integrity and Confidentiality should be maintained:** Investigators should carry out investigations lawfully and with integrity, and confidentiality (ACPO, 2012; Srinivasan, 2007).	P11	IC10	Integrity
E11	**Consideration for the well being of investigators** as highlighted by Burruss, *et al.* (2018).			Social Responsibility

Table 4: List of Ethical Principles to Inform Forensics Investigations.

6. The Tensions

A trusting relationship between citizens and state is built on the assumption that government will legitimately gather personal information to undertake the administration of state activities or for national security reasons (Whitley, 2009). In addition, democratic governments need to trust that most of their citizens are law abiding and can be left to get on with their lives. The balance of this relationship requires respect for the right to freedom, choice and maintaining democracy for citizens alongside the government's civic duty to administer, govern and protect (Lenoble and Maesschalck, 2003). This aligns well with Rawls' principles of liberty and equality. The limits to government's power guarantee the citizen certain rights and freedoms, and ensure that there can be justice for all.

Yet there are tensions. On the one hand, there is an expectation of almost 100% security for personal transactions such as banking, medical records, and conversations with loved ones, whilst, on the other, there is an expectation of full access to carry out digital forensics investigations into the records of criminals and terrorists by investigators (Solove, 2001).

Governments are in the unenviable position of having conflicting dual roles: being both guardians of privacy legislation (Bischoff, 2018, EU Parliament, 2018) and overseers of investigative agencies, at the same time. The former role requires them to restrict access to personal information, while the latter urges extensive harvesting of potentially personal or organizationally-sensitive information. What we have, in reality, is a circle that is very difficult to square.

6.1. Law Enforcement & Security Needs

The difficulties forensic investigators face is clear. They walk the tightrope between protecting and violating citizens' privacy during their labors. This is made more difficult by a lack of agreement about the definition of privacy, on the one hand, and the ability to know when our privacy has been violated, on the other. Governments, too, face a conundrum. They react to perceived threats by implementing ever more complex and covert surveillance, and enact privacy-invasive legislation (Section 6.1.1). Citizens react by adopting ever more sophisticated privacy-protecting technologies, preventing government surveillance (Section 6.1.2).

6.1.1. Surveillance:

Governments call for greater and often more intrusive surveillance measures in order to protect citizens and provide them with a greater perception of safety and security. Yet there is a danger that, as Ben Franklin stated "*Those who would give up essential Liberty, to purchase a little temporary safety, deserve neither liberty nor safety*". The force of argument coming from the security industry, however, is often emotionally charged with scenarios of death and disaster that could have been avoided by using their new tool or surveillance system. Politicians, the media and the security industry often promote fear of crime, terrorism and national security threats to sell ever more sophisticated surveillance and security technologies (Mueller, 2006). The loss of privacy and freedom that such technologies constitute appears to be ignored.

Yet countries in Europe do not have unlimited discretion to put their citizens under surveillance. European Courts have ruled that States may not adopt measures that are disproportionate to the right to privacy, even in the name of counter-terrorism or organized crime (Limitations of Rights, 1978). The UK's Investigatory Powers Act (IPA) (UK Government, 2016) breaches this, and the national security argument is used to justify it. There is a surprising lack of any mainstream backlash (Renaud *et al.*, 2016).

6.1.2. Dark Clouds:

In parallel to the increasing sophistication and capability of digital investigations to uncover evidence, mechanisms designed specifically to preserve privacy have also become increasingly popular. This counters the efforts of forensics investigators (Ferguson *et al.*, 2018). The privacy-preserving mechanisms include encryption, full disk encryption using tools such as VeraCrypt or Bitlocker, secure network communication using Virtual Private Networks, Secure Processors, homomorphic encryption (Gentry, 2009) and anonymous routing using TOR (Reed *et al.*, 1998). Cyber criminals are becoming particularly adept at preventing forensics investigators from uncovering evidence of their activities by deploying many of these mechanisms (Nouh *et al.*, 2019).

The improvements in cyber security, privacy-preserving tools and encryption could be leading us towards a future information blackout for those who carry out digital forensics investigations. Evidence that this is starting to happen includes:

a) The move away from advice to first responders to simply 'pull the plug' (thereby losing provided encryption keys) to the use of live imaging techniques rather than the more forensically sound static techniques (Voorhees, 2017).

b) The FBI-Apple dispute (Grossman, 2016) over access to encrypted data on iPhone devices shows that the encryption techniques used in consumer devices are now sufficiently strong to prevent law-enforcement access without the cooperation of the manufacturer. However, the San Bernadino Terrorist case (Tanfani, 2018) demonstrates that defects in the implementation of the encryption technology could still be exploited to allow access.

c) The VPN market has grown dramatically, as analyzed by Statista[3], which demonstrates current and predicts future widespread adoption of communications encryption by the average citizen.

d) The increase in the number of ToR nodes from around 2000 in 2010, to between 6000-7000 in 2019[4], also reveals an uptake in privacy-preserving technologies.

Security services and law enforcement are aware of the way these privacy-preserving technologies are starting to prevent them from gathering digital evidence. Some governments and law enforcement agencies have responded by demanding access to privately held information and the ability to decrypt information (Ingersoll, 2013, Vaas, 2019).

The *Five Eyes* countries, the intelligence alliance of Australia, Canada, New Zealand, the UK and the USA (Tossini, 2017), are demanding access to encryption keys (Blanchard, 2017; Afifi-Sabet, 2018; Cuthbertson, 2017; Newman, 2018), with Australia enacting legislation to mandate that companies divulge their keys (The Straits Times, 2018). The FBI in the USA refers to encryption as a 'major public health issue' (Nakashima, 2018). The outcome will be systems that are vulnerable to hackers, thereby reversing any security benefits that encryption and other such tools currently deliver.

Law enforcement is also increasingly demanding that software companies insert "back doors" (Cox, 2019, Dormehl, 2016): secret entrances designed into the system. The problem is that such backdoors will not remain secret. They are likely also to offer an entry to hackers, and are aptly named "back doors" because they let people in while the defenders are occupied securing the most obvious entry point: the front door. Some companies are defying government demands for backdoors (Talwar, 2019; Owen, 2018).

Further, it is understood that those who engage in criminal or terrorist activities are likely to be aware of the security services' attempts to monitor them, and so use advanced (or offline) techniques to hide their communications. Therefore, those with the least to hide are also those who are the most surveilled, leaving the security services with largely the same problems as before. It is the criminals and terrorists who are the most adept at providing false trails, using proxies and finding ways to circumvent the security services, whilst the noise and chatter from mass surveillance is in danger of enabling criminals to hide in plain sight.

Whilst the 'Dark Clouds' identified by Ferguson *et al.* (2018) constitute the main threat to the continued success of the digital forensics discipline, they are not the only difficulties faced by forensics practitioners. A further 'Grey Cloud' exists (GC in Table 5) comprising of familiar *anti-forensic techniques* including: (1) artifact-wiping via file-wiping, (2) artifact-wiping via disk-wiping, (3) artifact-wiping via log-wiping, (4) data-hiding via vault app, (5) data-hiding via proxy server, (6) data-hiding via IP address-spoofing, (7) trail obfuscation via private browsing, and (8) trail obfuscation via e-mail encryption.

[3] https://www.statista.com/statistics/542817/worldwide-virtual-private-network-market/

[4] https://metrics.torproject.org/networksize.html?start=2010-06-26&end=2019-09-24

These measures, whilst not necessarily show stoppers for a given investigation, mandate the use of more complex, (thus slower and more expensive) digital forensic techniques.

Forensics investigators experience difficulties in understanding how to address these issues whilst still conducting their investigations and safeguarding communities from crime and terrorism. It is unsurprising that they may consider the integration of ethical considerations into their investigations a step too far, given the challenges these dark clouds already constitute. Table 5 enumerates four distinct "Dark Cloud" threats and one "Gray Cloud" threat to forensics investigations. We shall situate the former within our framework.

DC1	Full Disk Encryption	DC4	E2E Encryption, TOR
DC2	Memory Encryption	DC5	Secure Network Communication
DC3	File Level Encryption	GC	Anti-Forensics Techniques

Table 5: Dark Cloud (DCi) and Gray Cloud (GC) Challenges

6.2. Individual Privacy Rights

Most countries give their citizens personal privacy rights – at least on paper. Yet the right to privacy is viewed by some governments as unimportant (Liberty, 2017; Pool and Custers, 2017; Barbaro, 2017). In part, this may be due to the difficulty in pinning down a definition everyone can agree with. People may know what privacy means to them, without necessarily being able to articulate their understanding. Gross (1967) described this conundrum very well: "*Without difficulty we regularly recognise those situations in which a violation of privacy is threatened or accomplished, yet stumble when trying to make clear what privacy is*" (p. 35). Gross (1967) quotes Hart (1954) who says: "*We can know yet not understand*". This might explain why people do not seem to object when their privacy is taken away from them, even if they feel a sense of unease (Renaud *et al.*, 2016).

This makes our privacy rights somewhat easier to discount or to minimize in perceived importance. Whilst we may be willing to accept that criminal investigations might need to sacrifice the individual's right to privacy, this should arguably not extend to violating an entire nation's privacy in the name of national security. UK and European law already has many rigorous measures in place to ensure that the individual's rights are respected. Governments put a great deal of effort into persuading citizens to take their privacy seriously, and they pass laws, such as GDPR (European Union, 2018), to ensure that organizations do so too. Yet, at the same time, they themselves want to be able to access people's data. Many, specifically the UK, now permit intrusions into people's digital lives without any judicial oversight (Big Brother Watch, 2018).

The old adage, still brought out by the state, the police or any other interested party: '*if you are doing nothing wrong…*' serves to remind us that their desire is to protect us from bad people and that good and law-abiding citizens have nothing to fear from the surges in surveillance or erosion of privacy via the collection and analysis of personal and often sensitive data. Such widespread surveillance undermines the legal presumption of innocence underlying legal process in our society (Milaj and Bonnici 2014), and violates Rawls' equality principle. The problem with this approach is that its adversarial and accusatory tone serves to reduce the debate to one whereby advocates of security 'for your safety' will accuse those voicing concern as being 'on the side of the criminals' thus stifling dissenting voices.

The situation is one in which governments are in the uncomfortable position of having conflicting dual roles: being both guardians of privacy legislation and overseers of investigative agencies at the same time. The former role requires them to restrict access to personal information, while the latter urges extensive harvesting of potentially personal or organizationally sensitive information.

6.3. Organizational Intellectual Capital Confidentiality

Forensics investigations can impact the three intellectual capital related assertions in Section 4.2 as follows:

(a) *Intellectual capital is valuable*: IC is valuable to organizations in terms of contributing towards future health and prosperity (Maditinos *et al.* (2000); Abeysekera (2006); Edvinsson, and Sullivan (1996)). It might be valuable to forensics investigators in another way i.e. to help them to join all the dots in their investigation. The tension here is that the value of IC to the latter might compromise the value to the former if such IC needs to be kept confidential.

(b) *IC disclosure should be controlled:* Organizations' intellectual capital can certainly be damaged by the activities of hackers (Snyder and Crescenzi, 2009). Consider, as an example, the Sony hack (Siboni and Siman-Tov, 2014). A number of unreleased movies were stolen. The hackers demanded money to return the movies. This was essentially a loss of Sony's intellectual capital and it is estimated that this cost Sony $35 million in IT repairs (Hornyak, 2015).

Our argument is that the activities of forensics investigators could also, inadvertently, damage intellectual capital. Beebe (2009) points to the mismatch between the data collection activities of digital forensics investigators and organizations' own policies and procedures for gathering data. This seems to be particularly applicable to tangible intellectual capital archives, which the organization may well want to keep out of the investigation, but which the investigator may wish to gain access to, in order to carry out an exhaustive investigation (*IG1*).

La Torre *et al.* (2018) warn against the "voracity" of big data, and the risk this poses to the intellectual capital of an organization. Yet forensics investigations are also potentially voracious as they attempt to gather all the information to be able to make a recommendation to a court of law.

(c) *If IC is leaked, or disclosure is uncontrolled, it could damage the organization*: If a digital investigator decides to pursue a particular line of enquiry, he or she is required, according to the *IG1* guideline in Table 1, to investigate exhaustively. Moreover, the investigator is also required to record all information, whether it be confidential or not (*IG4*), and to make intangible information tangible (*IG5*), in terms of recording it. Such recorded information could conceivably be presented in court, and the organization has lost the ability to control disclosure. In effect, a forensics investigation, unconstrained by considerations of investigation scope and remit, might result in uncontrolled disclosure, which could feasibly damage the organization's intellectual capital and their future potential to thrive.

6.4. Mapping Ethics to Investigation Guidelines

Ethical Principle	**aligns (✔) opposes (✖)**	**Investigative Guideline**
E1: Delineate Remit	✖	IG1: Exhaustively investigate
E2: Respect the privacy of the subject	✖	IG2: Comprehensively record all information
E3: Only investigate other parties if there is evidence of their involvement	✖	IG3: Investigate all relevant related parties
E4: Bookmark and exclude private information	✖	IG4: Sensitive material should be recorded but marked as such
E5: Document all actions	✔	IG5: Record intangible information
E6: Facilitate audits	✔	IG6: Give prosecutor record of gathered information
E7: Report all investigative activities	✔	IG7: Retain all information
E8: Be transparent about the extent of the investigation, and the gathered information	✔	IG8: Allow accused to inspect information
E9: Investigators should undergo regular training	✔	IG9: Investigators must be competent to report on investigation

E10: Information's Integrity and Confidentiality should be maintained	✔	IG10: Information Integrity should be maintained:
E11: Consideration for the well being of the investigator/s		

Table 6: Mapping Ethical Principles (*Ei*) to Investigative Guidelines (*IGi*)

It is now possible to map the investigative guidelines outlined in Table 1 to the ethical principles outlined in Table 4. Table 6 depicts the tensions between the privacy expectations of citizens and organizations and the information gathering desires of governments and law enforcement. As you can see, ethical principles E1, E2, E3 and E4 do not align with current investigative guidelines.

6.5. The Sweet Spot?

The danger being faced is that a desire for total safety and security, operationalized without adequate checks and balances, particularly if individual freedoms fail to be preserved, may ultimately result in a dystopian society where individuals have neither liberty nor equality. In the next section, the PRECEPT privacy-respecting framework is proposed to inform ethical digital forensics investigations that will ensure that society does not end up at the top left-hand corner of Figure 2. Yet the bottom right-hand corner is equally unrealistic and infeasible, given the legitimate needs of our law enforcement bodies. The proposed framework aims to inform digital investigations while balancing these tensions

7. PRECEPT

A number of digital forensics investigative stages have been proposed in the literature; a selection of these are compared and contrasted in Table 8 in the Appendix. All the stages in the left-most column have been retained except that of proof/defense because, in our view, this is not part of the investigation process – it occurs after the investigation has concluded.

Pollitt (2016) argues for the importance of planning in successful forensics investigations. He suggests that formulating a number of questions that guide the forensics investigator as the investigation is proceeding. Ieong (2006) proposes six specific questions along these lines: *What* (the data), *Why* (the motivation), *How* (the procedures), *Who* (the people), *Where* (the location), and *When* (the time). These questions, Pollitt (2016) argue, help the investigator to bridge the physical investigation and the digital world of evidence being explored. Our framework addresses one particular question, "the how", while the investigator seeks to answer the other questions during their investigation.

A brief explanation of the PRECEPT stages is provided in Table 7 (Stages referred to as *Si*).

7.1. Expert Review

Phase 1

An expert review was carried out, as advised by Mack and Nielsen (1995). The framework diagram was sent to 6 forensics investigators (2 academics and 4 practitioners), together with the questionnaire provided in Appendix A. The questions were essentially qualitative in nature and the responses from the small number of experts do not support any quantitative analysis. There were a number of comments related to the need to be able to launch a new investigation at any point, so we added the explanatory text in the box to reflect that. There were some comments about our descriptions of the stages, which helped us to improve the explanations in Table 7. Two argued that acquisition should come after preservation, but this misunderstanding was due to a suboptimal description of these stages in our explanations, which we have now improved. Another two said they did not usually engage in reconstruction, but they did not object to its inclusion in the framework.

One of the expert reviewers, a policeman, said, when referring to identification: "*Must understand the possibility of residual data (personal details of persons other than the suspect and whether there is a right to inspect those details)*". The same policeman said, with respect to search: "*It all links back to the agreed scope of the investigation and the risk associated with examining the data*". Another reviewer made a point of emphasizing the need to delineate the examination scope at the outset. Only minor tweaks were made to the original framework based on their feedback.

Phase 2

We subjected the revised framework to further review by 14 forensics investigators as an activity at a digital forensics workshop. These investigators were given the diagram, the list of ethical principles and the list of dark cloud issues. They were asked to complete the questionnaire provided in Appendix A, and provided their feedback.

Based on their responses we added a new ethical principle: "*E11: Consideration for the well being of the investigator/s*" This was mentioned by a number of evaluators during the workshop, and led to a lively discussion. We expanded S8 to include the considered discarding of irrelevant evidence that had been collected during the course of the investigation. S8 now also includes a reflection related to identifying the need for support for investigators who might have been traumatized by the investigation. One expert highlighted the need to have a record of the investigators who had been involved in the investigation, together with a description of their activities, which is now included in the stage S8. We also removed E3 from the S1 stage, given the argument by two evaluators that it was not possible to identify the subject in many cases so early in the process. We added E4 to the S4 stage, based on two evaluators arguing that it would not be possible to remove irrelevant information in S8 without the investigator having done this in the earlier stages. Finally, a number of the evaluators suggested that we include some color in the diagram to make it easier for the reader to identify similar concepts. This also makes the "dark clouds" more salient.

The final refined PRECEPT framework is presented in Figure 4.

7.2. Discussion

The PRECEPT framework was developed to inform digital forensics investigations in such a way that it balances digital investigator needs and the privacy and confidentiality rights of individuals and organizations. The framework has been constructed by combining the stages of digital investigations and adding in the potential problems of changes in technology to the investigative process (the "Dark Clouds" Ferguson *et al.* (2018) refer to) and also taking into account the rights (in particular privacy) of individuals. The included premises have been derived from the extensive debate in the literature, standard investigative operating procedures, ethical principles and ethical dilemmas. The output from the framework is a report (taking into account the balance between digital investigator needs and ethical rights) that can be used for court as well as the information that a digital investigator can use if a court appearance is required.

As indicated earlier, the objective of the framework is to provide digital forensics practitioners with a structure to navigate the tensions and complex environment (both technical and ethical) within which digital investigations take place. The framework seeks to take into account the challenges in digital investigations created by the development of new technologies and secure digital platforms, indicated by red crosses on the framework diagram. The framework highlights the dilemmas (ethical and otherwise) between security and privacy in the context of digital investigations. The framework is set in the context of ethical principles and how these should be used to shape digital investigations. In essence, this discussion sought to portray the balance between the technical and legal requirements associated with digital investigations, the privacy of individuals and the ethical rights of society.

PRECEPT uses the "life cycle" of a digital investigation from identification through to reporting (the spine in the framework diagram derived from the UK's Core Investigative Doctrine 2015), and contextualizes the challenges and issues at each stage utilizing the components and ethical principles derived from the Criminal Procedure and Investigations Act (1996).

PRECEPT aligns the ethical principles (referring to the principles in Table 4) with the various stages of the framework. By embedding the principles at the relevant stages in the process, the focus is to encourage the digital investigators to consider the principles in addition to the technical and legal aspects at each stage. By making these suggestions in the framework, the authors attempt to encourage digital forensics investigators and practitioners to broaden their investigations and take at each of the identified stages into account during the investigation process.

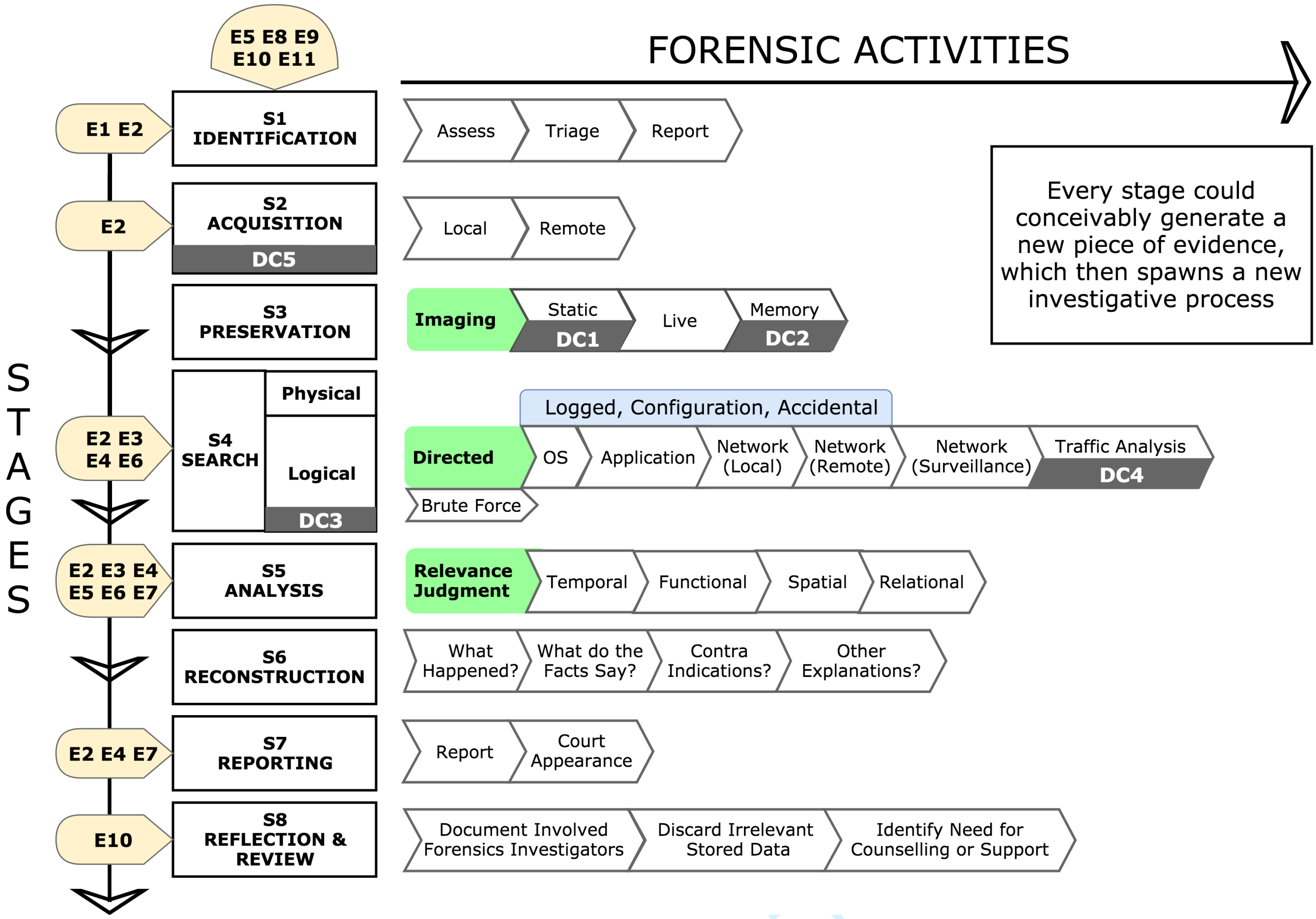

Figure 4: **PRECEPT**: Privacy-Respecting Forensics Investigation Framework
(S*i* refers to investigation stages in Table 7, DC*i* refers to challenges to digital investigations i.e. “Dark Clouds” listed in Table 5; E*i* refers to the ethical principles outlined in Table 4).

8. CONCLUSION

This paper draws on the privacy, intellectual capital, investigative guidelines, ethics, anti-forensics and forensics investigation stage literature to derive at an ethically-informed framework to guide digital forensics investigations. We subjected the derived framework to expert review and refined it accordingly. In proposing PRECEPT, we follow the recommendations of a number of researchers, who highlight the need for a privacy-protecting framework which balances the needs of investigators with the rights of individuals and organizations.

We hope that the PRECEPT framework will launch a discussion into resolving these tensions and, most importantly, to ensure that Rawls’ two core principles of liberty and equality are respected and a societal sense of justice is to maximized. We plan to continue to refine the PRECEPT framework, based on feedback obtained from interested academics and practitioners in the field. The ultimate aim is to produce a helpful resource to forensics investigators, but also reassure the public that their privacy rights are indeed being respected and considered. We want to move towards satisfying the requirements of the Daubert test for the PRECEPT framework, and to establish a more equitable balance of power between the key stakeholders.

S1	***Identification***: Identifying that an incident has taken place – e.g. crime report, link from another investigation: a. *assess* – establish the crime scene(s) b. *triage & report* – rapid evaluation of situation and report on judgement
S2	***Acquisition***: Physical seizure and storage of devices and data – locally and remote – a. *local* - acquisition of locally held data b. *remote* - acquisition of data held on the Internet/Cloud/private networks
S3	***Preservation***: Copying and verification (check summing) of media i.e. making a forensic image: a. *static imaging* – lab-based – storage device (disk/chip removed). b. *live imaging* – i.e. crime scene: image store attached to target machine or over-the-network imaging. c. *memory imaging*
S4	***Search***: Recovery of data from physical media, including undeletion, decryption etc.: a. *physical search* – (1) search of binary images, (2) file carving, (3) searching in the absence of a file system. b. *logical search* – search of file system: i. *brute-force* – recovery of all material (e.g. all jpg). ii. *directed* – search led by knowledge of case. 1. OS – Evidence from the operating system: a. *configuration* – How was the system set up: devices, users, network, applications etc. b. *accidental* – Artifacts left by fundamental operation of device (e.g. spool files, pagefile.sys). c. *logged* – system logs. 2. Applications a. *configuration* – How was each application set up? e.g. default save directory. b. *accidental* – Artifacts left by fundamental operation - e.g. tmp files c. *logged* – e.g. error logs and transaction logs. 3. Network (local) – e.g. browser forensics, email, messaging: a. *configuration* – How was each network application set up? b. *accidental* – Artifacts left by fundamental operation - e.g. cache files c. *logged* – e.g. browser history. 4. Network (remote) – server and network devices (routers) a. *configuration* – How was each network device set up? b. *accidental* – Artifacts left by fundamental operation - e.g. routing tables, web-server logs. c. *logged* – e.g. dhcp/dns logs. 5. Network (surveillance) – packet sniffing, ISP cooperation: a. *Traffic analysis* – If traffic is encrypted, then source/destination, timestamp and volume information may still be available.
S5	***Analysis***: relevance judgments, organization of low-level facts into evidence: four semi-orthogonal concerns: temporal, spatial, relational, functional a. *Functional* – What happened? Who did what? b. *Temporal* – When or in what order did things happen? c. *Spatial* – Where did things happen? d. *Relational* – What items of interest are related to others and how?
S6	***Reconstruction***: hypotheses induction and testing. Equivocal analysis. a. What do you think happened? b. How can it be supported from the facts? c. What contra-indications are there? d. Alternative explanations?
S7	***Reporting***: Court report, court appearance.
S8	***Reflection & Review***: Consideration of performance and lessons to be learned. a. Produce a document detailing which forensics investigators were involved, and their specific activities, if possible. b. Discard irrelevant data that was acquired and preserved. c. Consider whether any of the investigators require support or counseling.

Table 7: Digital Forensics Investigation Stages

REFERENCES

Abeysekera, I. (2006), “The project of intellectual capital disclosure: researching the research", *Journal of Intellectual Capital*, Vol. 7 No. 1, pp. 61-77,

ACM Committee on Professional Ethics. (2018), “*ACM Code of Ethics and Professional Conduct*”, available at: https://ethics.acm.org/, (accessed 18 April 2019).

ACPO (Association of Chief Police Officers). (2012), "*ACPO Good Practice Guide for Digital Evidence*", available from: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (accessed 27 April 2019).

Adams, J.S. (1965), "Inequity in social exchange", *Advances in Experimental Social Psychology,* Vol. 2, pp. 267-299.

Adams, R. (2012), "*The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice*", PhD thesis, School of Information Technology, Murdoch University.

Afifi-Sabet, K. (2018), "*Industry given final warning as governments declare they are ready to legislate for backdoor access*", available at: https://www.itpro.co.uk/encryption/31822/five-eyes-nations-hand-tech-giants-encryption-ultimatum (accessed 10 April 2019).

Agarwal, R. and Kothari, S. (2015), "Review of digital forensic investigation frameworks", In *Information Science and Applications* (pp. 561-571). Springer, Berlin, Heidelberg.

American Psychological Association. (2016), "*Ethical Principles of Psychologists and Code of Conduct*", available at: http://www.apa.org/ethics/code/index.aspx (Accessed 18 May 2018).

Aminnezhad, A., Dehghantanha, A., and Abdullah, M. T. (2012), "A survey on privacy issues in digital forensics", *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, Vol. 1, pp. 311–323.

Anderson, R.E., Johnson, D.G., Gotterbarn, D. and Perrolle, J. (1992), "*ACM code of ethics and professional conduct*", *Communications of the ACM,* Vol. 35 No. 5, pp. 94-99.

Antoniou, G., Wilson, C. and Geneiatakis, D. (2006) "PPINA – A Forensic Investigation Protocol for Privacy Enhancing Technologies", In *Proceedings of the 10th IFIP on Communication and Multimedia Security*, pp. 185-195,

Cuthbertson, A. (2017), "*FBI Chief Says Encryption Is 'Huge Problem'*", 23 October, available at: https://www.newsweek.com/fbi-encryption-christopher-wray-apple-whatsapp-690523 (accessed 8 April 2019).

Balogun, A.M. and Zuva, T. (2017), "Open Ethical Issues In Digital Forensic Systems", *International Journal of eBusiness and eGovernment Studies*, Vol. 9 No. 1, pp. 55-69.

Barbaro, M. (2017), "Government Interference with the Right to Privacy: Is the Right to Privacy an Endangered Animal", *Canadian Journal of Human Rights*, Vol. 6, pp. 127-153.

Barendt, E. (Ed.). (2001), *Privacy*, London: Routledge, https://doi.org/10.4324/9781315246024

Barney, J. (1991), "Firm Resources and Sustained Competitive Advantage", *Journal of Management*, Vol. 17 No. 1, pp. 99-120.

Beebe, N. (2009), "Digital forensic research: The good, the bad and the unaddressed", In *IFIP International Conference on Digital Forensics* (pp. 17-36). Springer, Berlin, Heidelberg.

Bennett, C. (1992), *Regulating Privacy,* Ithaca: Cornell University Press.

Big Brother Watch. (2018), "*The State Of Surveillance In 2018*", available at: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/09/The-State-of-Surveillance-in-2018.pdf (accessed 8 April 2019).

Big Brother Watch. (2019), "*Campaigners denounce "abject failure" of police to reform digital investigations of rape victims*", available at: https://bigbrotherwatch.org.uk/all-media/campaigners-denounce-abject-failure-of-police-to-reform-digital-investigations-of-rape-victims/ (accessed 25 September 2019).

Bischoff, P. (2018), "*Which US states best protect privacy online?*", available at: https://www.comparitech.com/blog/vpn-privacy/which-us-states-best-protect-online-privacy/ (accessed 25 September 2019).

Blanchard, J. (2017), "*Government eyes new laws for clampdown on encryption of WhatsApp messages in wake of London terror attack*", available at: https://www.mirror.co.uk/news/politics/government-eyes-new-laws-clampdown-10105142 (accessed 10 April, 2019).

Blum, D. (2006), "Making Business Sense of Information Security", *Security and Risk Man*agement *Strategies In-Depth Research Overview*, available at: https://cse.sc.edu/~buell/References/ComputingHigherEdMisc/ERS0601.pdf (accessed 29 April 2019).

Brennan, N. (2001), "Reporting intellectual capital in annual reports: evidence from Ireland", *Accounting, Auditing & Accountability Journal*, Vol. 14 No. 4, pp. 426-436.

Brown, A., Osborn, T., Chan, J.M. and Jaganathan, V. (2005), "Managing intellectual capital", *Research-Technology Management*, Vol. 48 No. 6, pp. 34-41.

Brown, W., (2000) "Ontological Security, Existential Anxiety and Workplace Privacy." *Journal of Business Ethics,* Vol. 23, pp. 61–65.

Burruss, G.W., Holt, T.J. and Wall-Parker, A. (2018), "The hazards of investigating internet crimes against children: Digital evidence handlers' experiences with vicarious trauma and coping behaviors", *American Journal of Criminal Justice*, Vol 43 No. 3, pp. 433-447.

Casciani, D. (2019), "*Zain Qaiser: Student jailed for blackmailing porn users worldwide*", 9 April, available at: https://www.bbc.co.uk/news/uk-47800378 (accessed 22 April 2019).

Casey, E. (2000), *Digital Evidence and Computer Crime*, San Diego: Academic Press.

Caviglione, L., Wendzel, S. and Mazurczyk, W. (2017), "The future of digital forensics: Challenges and the road ahead", *IEEE Security & Privacy*, Vol. 15 No. 6, pp. 12-17.

CENTREX. (2005), "*Practice Advice on Core Investigative Doctrine*", available at: http://library.college.police.uk/docs/acpo/Core-Investigative-Doctrine.pdf (accessed 8 April 2019).

Chen, M. M.-C., Cheng, S. S.-J., and Hwang, Y. (2005), "An empirical investigation of the relationship between intellectual capital and firms' market value and financial performance", *Journal of Intellectual Capital*, Vol. 6 No. 2, pp. 159–176.

Ciardhuáin, S.Ó. (2004), "An extended model of cybercrime investigations", *International Journal of Digital Evidence*, Vol. 3 No. 1, pp. 1-22.

CIC. (2008), "*EFFAS Commission of Intellectual Capital Principles for Effective Communication of Intellectual Capital*", available at: https://effas.net/pdf/setter/EFFAS-CIC.pdf (accessed 11 April, 2019)

College of Policing. (2015), "*Revised cybercrime training for police*", available at: https://www.college.police.uk/News/archive/September_2015/Pages/Revised_cybercrime_training_for_police.aspx (accessed 25 September 2019).

College of Policing. (2014), "*Code of Ethics*", available at: https://www.college.police.uk/What-we-do/Ethics/Ethics-home/Documents/Code_of_Ethics.pdf (accessed 25 September 2019).

Cox, J. (2019), "*Barr Says Police Need Encryption Backdoors, Doesn't Mention Hacking Tools They Use All the Time*", available at: https://www.vice.com/en_us/article/neaadm/barr-says-police-need-backdoors-doesnt-mention-hacking-cellebrite-graykey (accessed 25 September 2019).

CPIA, (1996), "*Criminal Procedure and Investigations Act 1996*", available at: https://www.legislation.gov.uk/ukpga/1996/25/contents (accessed 8 April 2019).

Croft, N. J. and Olivier, M.S. (2010) "Sequenced release of privacy-accurate information in a forensic investigation," *Digital Investigation* Vol. 7, pp. 1-7.

Deacon, A. (1998) "Public Welfare And Private Behaviour: The Case Of 'Welfare To Work' Programmes", *Paper delivered to the 2nd International Research Conference of the International Social Security Association*, Jerusalem, available at: https://www.issa.int/html/pdf/jeru98/theme3/3-1b.pdf (accessed 9 April 2019).

de Bruijn, H. and Janssen, M. (2017), "Building cybersecurity awareness: The need for evidence-based framing strategies", *Government Information Quarterly*, Vol. 34 No. 1, pp. 1-7.

Dehghantanha, A. and Franke, K. (2014), "Privacy-respecting digital investigation", In *Twelfth Annual International Conference on Privacy, Security and Trust*, pp. 129-138.

Deng, M., Wuyts, K., Scandariato, R., Preneel, B. and Joosen W. (2010), "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements", *Requirements Engineering*, Vol. 16 No. 1, pp. 3–32.

Department of Health, Education, and Welfare. (1979), "*The Belmont Report*", available at: https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/#xrespect (Accessed 18 May 2018).

Deutsch, M. (1986), "Cooperation, conflict, and justice", In Bierhoff H.W., Cohen R.L., Greenberg J. (eds), *Justice in Social Relations. Critical Issues in Social Justice. Springer, Boston, MA,* pp. 3-18.

DFRWS. (2001), "*A Road Map for Digital Forensic Research by Collective work of all DFRWS attendees*" available at: http://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf (accessed 5 May 2019).

Dienlin, T., and Trepte, S. (2015), "Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors", *Eur. J. Soc. Psychol.*, Vol. 45, pp. 285– 297.

Digital Forensics Certification Board. (Undated), "*Code of Ethics and Standards of Professional Conduct*" available at: https://dfcb.org/code-of-ethics-and-standards-of-professional-conduct/ (accessed 8 April 2019).

Dormehl, L. (2016), "*FBI: iPhone backdoor would not set dangerous precedent, we promise*", available at: https://www.cultofmac.com/413639/fbi-iphone-backdoor-would-not-set-dangerous-precedent-we-promise/ (accessed 25 September 2019).

Du, X., Le-Khac, N.A. and Scanlon, M. (2017), "*Evaluation of digital forensic process models with respect to digital forensics as a service*", available at: https://arxiv.org/abs/1708.01730arXiv. (accessed 5 May 2019).

Dumay, J. (2016), "A critical reflection on the future of intellectual capital: from reporting to disclosure". *Journal of Intellectual capital*, Vol. 17 No. 1, pp. 168-184.

Dumay, J. and Guthrie, J. (2017), "Involuntary disclosure of intellectual capital: is it relevant?", *Journal of Intellectual Capital*, Vol. 18 No. 1, pp. 29-44.

Edvinsson, L. and Sullivan, P. (1996), "Developing a model for managing intellectual capital", *European Management Journal*, Vol. 14 No. 4, pp. 356-364.

Etzioni, A. (1997), "Balancing Individual Rights and the Common Good", *Tikkun, Vol.* 12 No. 1 Jan/Feb, pp. 66-67.

EU Parliament. (2018), "*Home Page of EU GDPR*", available at: https://www.eugdpr.org/(accessed 12 April 2019).

Fairweather, N. B. (2001), "Privacy in the Age of Bigger Brother". In *ETHICOMP, Gdansk*, pp. 309-317.

Ferguson, R.I., Renaud, K., Irons, A. (2018), "Dark Clouds on the Horizon The Challenge of Cloud Forensics". *IRIA Cloud Computing, Barcelona.*

Forensics Science Regulator, (2014) "*Codes of Practice and Conduct. Appendix: Digital Forensic Services. FSR-C-107. Issue 1*", available at: https://www.gov.uk/government/publications/digital-forensic-services-codes-of-practice-for-forensic-service-providers (accessed 8 April 2019).

Forester, T. and Morrison, P. (1995), *Computer Ethics: Cautionary tales and ethical dilemmas in computing*. Massachusetts: Massachusetts Institute of Technology.

Forgang, J.D. (2009), "The Right of the People: The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas", *Fordham Law Rev*iew, Vol. 78, pp. 217-239.

Gay, J.R. (2012), "A Code of Conduct for Computer Forensic Investigators", PhD thesis, Information Security, *University of East London*, available at: http://roar.uel.ac.uk/1787/1/2012_DInfSec_Gay.pdf (accessed 8 April 2019).

Gentry, C. (2009), "Fully homomorphic encryption using ideal lattices." *ACM Symposium on Theory of Computing*, Vol. 9 No. 2009, pp. 169–178.

Global Information Assurance Certification (GIAC) (undated) "*Code of Ethics*", available at: https://digital-forensics.sans.org/certification/ethics (accessed 8 April 2019).

Grobler, C.P., Louwrens, B., Eloff, J., Labuschagne, L., Eloff, M. and Venter, R. (2006), "Digital forensics: a multi-dimensional discipline", In *Proceedings of the ISSA 2006 from Insight to Foresight Conference*. Pretoria: University of Pretoria.

Gross, H. (1967), "The concept of privacy", *New York University Law Review*, Vol. 42, pp. 34-54.

Grossman, L. (2016), "Inside Apple CEO Tim Cook's Fight With the FBI", available at: https://time.com/4262480/tim-cook-apple-fbi-2/ (accessed 24 September 2019).

Gupta, A. (2013), “Privacy preserving efficient digital forensic investigation framework”, In *2013 Sixth International Conference on Contemporary Computing (IC3)* (pp. 387-392).

Guthrie, J. and Petty, R. (2000), “Intellectual capital: Australian annual reporting practices”, *Journal of Intellectual Capital*, Vol. 1 No. 3, pp. 241-51.

Halboob, W., Abulaish, M. and Alghathbar, K.S. (2011), “Quaternary privacy-levels preservation in computer forensics investigation process”, In *2011 International Conference for Internet Technology and Secured Transactions* (pp. 777-782).

Halboob, W., Mahmod, R., Udzir, N.I. and Abdullah, M.T. (2015), “Privacy Levels for Computer Forensics: Toward a More Efficient Privacy-preserving Investigation”, *Procedia Computer Science*, Vol. 56, pp.370-375.

Harrington, S. (2014), “*Professional Ethics in the Digital Forensics Discipline: Part 1*”, available at: https://www.forensicmag.com/article/2014/03/professional-ethics-digital-forensics-discipline-part-1 (accessed 25 September 2019).

Hornyak, T. (2015), “*Hack to cost Sony $35 million in IT repairs*” available at: https://www.networkworld.com/article/2879814/sony-hack-cost-15-million-but-earnings-unaffected.html (accessed 13 May 2019).

Ieong, R.S. (2006), “FORZA–Digital forensics investigation framework that incorporate legal issues”, *Digital Investigation*, Vol. 3, pp.29-36

Ingersoll, G. (2013) “*REPORT: NSA Asks For Encryption Keys That Could Allow It To ‘Live On The Network’*”, Available from: https://www.businessinsider.com/government-demands-encryption-keys-2013-7?r=US&IR=T (accesssed 24 September 2019).

Inkinen, H. (2015), “Review of empirical research on intellectual capital and firm performance”, *Journal of Intellectual Capital*, Vol. 16 No. 3, pp. 518–565.

Irons, A.D. and Konstadopoulou, A. (2007), “Professionalism in digital forensics”, *Digital Evidence & Elec. Signature Law Review*, Vol. 4 No. 2, pp. 65-71.

Irons, A.D., Stephens, P. and Ferguson, R.I. (2009), “Digital Investigation as a distinct discipline: A pedagogic perspective”, *Digital Investigation*, Vol. 6 No. 1-2, pp. 82-90.

ISO. (2011), “Information Technology—Security Techniques—Privacy Framework; ISO/IEC 29100:2011 Standard”, in *International Organization for Standardization (ISO)*: Geneva, Switzerland, 2011.

John, J.L. (2012), *Digital forensics and preservation*. York: Digital Preservation Coalition.

Karia, D. (2010), “Ethics in Computer Forensics”, *Digital Forensics Magazine*, No. 5, 1 November.

Karie, N.M. and Venter, H.S. (2015), “Taxonomy of challenges for digital forensics”, *Journal of Forensic Sciences*, Vol. 60 No. 4, pp. 885-893.

King, B.J. (2001), “Deliberative democracy expanded: balancing freedom of expression and hate propaganda within the "I & We" paradigm”, *Master of Arts Dissertation*, Legal Studies, Carleton University.

Klaila, D. and Hall, L. (2000), “Using intellectual assets as a success strategy”, *Journal of Intellectual Capital*, Vol. 1 No. 1, pp. 47-53.

Köhn, M.D., Eloff, M.M. and Eloff, J.H.P. (2013), “Integrated Digital Forensic Process Model”, *Computers & Security*, Vol. 38, pp. 103–115.

Kounadi, O., Bowers, K. and Leitner, M., 2015. “Crime mapping on-line: Public perception of privacy issues”, *European Journal on Criminal Policy and Research*, Vol. 21 No. 1, pp. 167-190.

Langheinrich, M. (2001), “Privacy by design—principles of privacy-aware ubiquitous systems”, In *International conference on Ubiquitous Computing*, pp. 273-291. Springer, Berlin, Heidelberg.

Laperche, B. J. (2016), “Large Firms’ Knowledge Capital and Innovation Networks” Knowledge Economy, pp.1-18. https://doi.org/10.1007/s13132-016-0391-7

La Torre, M., Dumay, J. and Rea, M.A. (2018), “Breaching intellectual capital: critical reflections on Big Data security”, *Meditari Accountancy Research*, Vol. 26 No. 3, pp.463-482.

Law, F.Y.W., Chan, P.F., Yiu, S.M., Chow, K.P., Kwan, M.Y.K., Tse, H.K.S. (2011), “Protecting digital data privacy in Computer Forensic Examination”, In *The 6th International Workshop on Systematic Approaches to Digital Forensic Engineering in conjunction with IEEE Security and Privacy Symposium (IEEE/SADFE 2011),* Oakland, CA.

Leal, C., Meirinhos, G., Loureiro, M. and Marques, C.S. (2017), “Cybersecurity Management, Intellectual Capital and Trust: A New Management Dilemma”, In *ECIC 2017-9th European Conference on Intellectual Capital*, pp. 171-183.

Lenoble, J. and Maesschalck, M. (2003), *Toward a theory of governance: the action of norms*, The Hague: Kluwer Law International.

Liberty. (2017), “*Government Concedes Need For Snoopers’ Charter To Protect Rights In Response To Tom Watson’s Landmark Legal Challenge – But Must Go Further*”, available from: https://www.libertyhumanrights.org.uk/news/press-releases-and-statements/government-concedes-need-snoopers%E2%80%99-charter-protect-rights (accessed 27 April 2019).

Lemos, R. (2007), “Teaching hacking helps students, professors say”, The Register, 7 August, available at: https://www.theregister.co.uk/2007/08/07/teaching_students_hacking/ (accessed 25 September 2019).

Locard, E. (1904), *L'enquête criminelle et les méthódes scientifiques*, Paris: E. Flammarion.

Longhetti, A. (1983), “Editorial”, *Journal of Forensic Sciences,* Vol. 28, pp. 3-5

Losavio, M., Seigfried-Spellar, K.C. and Sloan III, J.J. (2016), “Why digital forensics is not a profession and how it can become one”, *Criminal Justice Studies*, Vol. 29 No. 2, pp. 143-162.

Losavio, M., Pastukov, P. and Polyakova, S. (2015), “Cyber black box/event data recorder: legal and ethical perspectives and challenges with digital forensics”, *Journal of Digital Forensics, Security and Law*, Vol. 10 No. 4, pp. 43-58.

Macewan, N.F. (2008), “The Computer Misuse Act 1990: lessons from its past and predictions for its future”, *Criminal Law Review*, Vol. 12, pp. 955-967.

Mack, R.L. and Nielsen, J. (1995), "Usability Inspection Methods: Executive Summary", In: *Readings in Human Computer Interaction: Toward the Year 2000*, R.M. Baecker , Eds., Morgan Kaufmann, pp. 170–181.

Maditinos, D., Chatzoudes, D., Tsairidis, C. and Theriou, G. (2011), "The impact of intellectual capital on firms' market value and financial performance", *Journal of Intellectual Capital*, Vol 12 No. 1, pp. 132-151.

Margulis, S.T., (2003) "Privacy as a social issue and behavioral concept." *Journal of social issues*, Vol. 59 No.2, pp. 243-261.

Milaj, J. and Bonnici, J.P.M. (2014), "Unwitting subjects of surveillance and the presumption of innocence", *Computer Law & Security Review*, Vol. 30 No. 4, pp. 419-428.

Mill, J.S. (1869), *On liberty*. Boston: Longmans, Green, Reader, and Dyer.

Ministry of Justice. (2015), "*Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice*", available at: at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/447967/code-of-practice-approved.pdf (accessed 8 April 2019).

Mitrović, A. and Knețević, S. (2016), "Specifics of financial reporting in special hospitals in Serbia", In *Proceedings: Tourism In Function Of Development Of The Republic Of Serbia*, pp. 157-172.

Mohamed, S., Mynors, D., Grantham, A., Walsh, K. and Chan, P. (2006), "Understanding one aspect of the knowledge leakage concept: people", In *Proceedings of the European and Mediterranean Conference on Information Systems (EMCIS),* pp. 6-7.

Moor, J. (2006), "Why we need better ethics for emerging technologies", *Ethics and Information Technology,* Vol. 7, pp. 111–119.

Mouritsen, J., Larsen, H.T. and Bukh, P.N. (2001), "Valuing the future: intellectual capital supplements at Skandia", *Accounting, Auditing & Accountability Journal*, Vol. 16 No. 4, pp. 399-422.

Nakashima, E. (2018), "*FBI chief calls encryption a 'major public safety issue*'", 9 January, availanle at: https://www.washingtonpost.com/world/national-security/fbi-chief-calls-encryption-a-major-public-safety-issue/2018/01/09/29a04166-f555-11e7-b34a-b85626af34ef_story.html (accessed 8 April, 2019).

Newman, L. H. (2018), "*Ag Rod Rosenstein Is Still Calling For An Encryption Backdoor*", 29 November, available at: https://www.wired.com/story/rod-rosenstein-encryption-backdoor/ (accessed 8 April, 2019).

Nieto, A., Rios, R. and Lopez, J. (2018), "IoT-Forensics meets privacy: towards cooperative digital investigations", *Sensors*, Vol. 18 No. 2 No. 492.

Nikkel, B.J. (2014), "Fostering incident response and digital forensics research", *Digital Investigation*, Vol. 11 *No.* 4, pp. 249-251.

NIST. (2014), "Cloud Computing Forensic Science Challenges", *National Institute of Standards and Technology Interagency or Internal Report 8006*, June.

Nouh, M., Nurse, J.R., Webb, H. and Goldsmith, M. (2019), "Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement", In *Proceedings of the Workshop on Usable Security (USEC) at Network and Distributed System Security Symposium (NDSS)*, February. San Diego.

NPCC. (2019), "NPCC comments on Big Brother Watch report suggesting changes to the new digital evicence consent forms", available at: https://news.npcc.police.uk/releases/npcc-comments-on-big-brother-watch-report-suggesting-changes-to-the-new-digital-evicence-consent-forms (accessed 25 September 2019).

Obeidat, B.Y., Abdallah, A.B., Aqqad, N.O., Akhoershiedah, A.H.O.M. and Maqableh, M. (2017), "The effect of intellectual capital on organizational performance: The mediating role of knowledge sharing", *Communications and Network*, Vol. 9 No. 1, pp. 1-27.

O'Driscoll, A. (2018), "*What is the Computer Fraud and Abuse Act?*" available at: https://www.comparitech.com/blog/information-security/computer-fraud-and-abuse-act/ (accessed 25 September 2019).

O'Neill, O. (1993), "Kantian ethics" In: *A companion to Ethics*, 29, pp. 175-85.

Officer.com. (2019), "*Overcome the Challenges of Digital Evidence*", available at: https://www.officer.com/investigations/forensics/digital-forensics/article/21090279/overcoming-the-challenges-of-digital-evidence (accessed 25 September 2019).

Orwell, G. (1949) *Nineteen Eighty-Four: A Novel*. London: Secker & Warburg.

Owen, M. (2018), "*Apple joins other tech giants denouncing Australia encryption backdoor proposals*," 3 October, available at: https://appleinsider.com/articles/18/10/03/apple-joins-other-tech-giants-denouncing-australia-encryption-backdoor-proposals, (accessed 10 April 2019).

Oyez. (2018), "*Carpenter v. United States*", available from: www.oyez.org/cases/2017/16-402 (accessed 26 September 2019).

Patterson, D.A. (2005), "20th century vs. 21st century C&C: the SPUR manifesto", *Communications of the ACM,* Vol. 48 No. 3, pp. 15-16.

Pollitt, M. (2016), "The key to forensic success: examination planning is a key determinant of efficient and effective digital forensics", *Digital Forensics* Chapter 2, (pp. 27-43). Syngress.

Pool, R.L.D. and Custers, B.H.M. (2017), "The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime", *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 25 No. 2, pp. 123-144.

Rawls, J. (1991), "Justice as fairness: Political not metaphysical", In *Equality and Liberty,* London: Palgrave, pp. 145-173.

Reed, M. G., Syverson, P. F. and Goldschlag, D. M. (1998) "Anonymous connections and onion routing," *IEEE Journal on Selected areas in Communications*, Vol. 16 No. 4, pp. 482–494.

Reith, M., Carr, C. and Gunsch, G. (2002), "An Examination of Digital Forensic Models", *International Journal of Digital Evidence*, Vol. 1 No. 3, pp. 1-12.

Renaud, K., Flowerday, S., English, R. and Volkamer, M. (2016), "Why don't UK citizens protest against privacy-invading dragnet surveillance?", *Information & Computer Security*, Vol. 24 No. 4, pp. 400-415.

Renaud, K. and Zimmermann, V. (2018), "Ethical Guidelines for Nudging in Information Security & Privacy", *International Journal of Human Computer Studies*, Vol. 120, pp. 22-35.

Rogers, M.K., Goldman, J., Mislan, R., Wedge, T. and Debrota, S. (2006), "Computer forensics field triage process model", *Journal of Digital Forensics, Security and Law*, Vol. 1 No. 2, pp. 19-38.

Rössler, B. (2005), *The value of privacy*. Cambridge, MA: Cambridge University Press.

Roux, B. and Falgoust, M. (2012), "Ethical issues raised by data acquisition methods in digital forensics research", *Journal of Information Ethics*, Vol. 21 No. 1, pp. 40-60.

Rule, J.B. (1973), *Private Lives and Public Surveillance*. London:Allen Lane.

Saleem, S., Popov, O. and Bagilli, I. (2014), "Extended abstract digital forensics model with preservation and protection as umbrella principles", *Procedia Computer Science*, Vol. 35, pp. 812-821.

Schoeman, F.D. (Ed) (1984), *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: University of Cambridge Press.

Sciulli, Nick, Wise, Victoria, Demediuk, Peter, Sims, Rob. (2002), "Intellectual Capital Reporting: An Examination of Local Government in Victoria", *Accounting, Accountability & Performance*, Vol. 8 No. 2, pp. 43-60.

Scott-Hayward, C.S., Fradella, H.F. and Fischer, R.G. (2015), "Does privacy require secrecy: Societal expectations of privacy in the digital age." *American Journal of Criminal Law*, Vol. 43, pp. 19-42.

Seigfried-Spellar, K.C. and Rogers, M. (2017), "Development of A Professional Code of Ethics in Digital Forensics", *Annual ADFSL Conference on Digital Forensics, Security and Law*, Daytona Beach, Florida, pp. 135-144.

Sharevski, F. (2015), "Rules of professional responsibility in digital forensics: A comparative analysis", *Journal of Digital Forensics, Security and Law*, Vol. 10 No. 2, pp. 39-54.

Siboni, G., Siman-Tov, D. (2014), "Cyberspace Extortion: North Korea versus the United States", *INSS Insight*, No. 646 http://www.inss.org.il/publication/cyberspace-extortion-north-korea-versus-the-united-states/, (accessed 7/1/2019)

Sloan, J. J. (2015), "There's no code of ethics to govern digital forensics – and we need one", *The Conversation. 10 August,* available at: https://theconversation.com/theres-no-code-of-ethics-to-govern-digital-forensics-and-we-need-one-45755 (accessed 8 April, 2019).

Snyder, Herbert. and Crescenzi, Anthony. (2009), "Intellectual capital and economic espionage: new crimes and new protections", *Journal of Financial Crime,* Vol. 16 No. 3, pp. 245-254,

Solove, D.J. (2001), "Privacy and Power: Computer Databases and Metaphors for Information Privacy", *Stanford Law Review*, Vol. 53 No. 6, pp. 1393-1462.

Sorell, T. and Draper, H. (2012), "Telecare, surveillance, and the welfare state", *The American Journal of Bioethics*, Vol. 12 No. 9, pp. 36-44.

Srinivasan, S. (2007), "Security and privacy vs. computer forensics capabilities". *Information Systems Control Journal*, Vol. 4, pp. 1-3.

Stahl, B., Elizondo, D., Carroll-Mayer, M., Zheng, Y. and Wakunuma, K. (2010), "Ethical and legal issues of the use of computational intelligence techniques in computer security and computer forensics", In *The 2010 International Joint Conference on Neural Networks (IJCNN),* Barcelona, Spain, pp. 1-8.

Strohm, C. (2017), "*Privacy Vs. Security*", available at: https://www.bloomberg.com/quicktake/privacy-vs-security (accessed 25 September 2019).

Swarb.co.uk. (2019) "REGINA V GOLD AND SCHIFREEN: CACD 17 JUL 1987", March 12, available at: https://swarb.co.uk/regina-v-gold-and-schifreen-cacd-17-jul-1987/ (accessed 24 September 2019).

Talwar, S. (2019) "*Fight for privacy: Why WhatsApp's reported plan to deny the government access to user chats is good news*", 27 March, available at: https://www.timesnownews.com/technology-science/article/fight-for-privacy-why-whatsapps-reported-plan-to-deny-the-government-access-to-user-chats-is-good-news/389793 (accessed 10 April 2019)

Tanfani, J. (2018), "Race to unlock San Bernardino shooter's iPhone was delayed by poor FBI communication, report finds", *The Los Angeles Times*, available at: https://www.latimes.com/politics/la-na-pol-fbi-iphone-san-bernardino-20180327-story.html (accessed 24 September 2019).

The British Psychological Society. (2014), "*Code of human research ethics*", available at: https://www.bps.org.uk/news-and-policy/bps-code-human-research-ethics-2nd-edition-2014 (accessed 18 May 2018).

The International Society of Forensic Computer Examiners (ISFCE) (2019), "*Code of Ethics and Professional Responsibility*" available at: https://www.isfce.com/ethics2.htm (accessed 8 April 2019).

The Investigator (undated), "How Google search history and Facebook posts are putting people in prison", available at: https://www.the-investigator.co.uk/websites#! (accessed 26 September 2019).

The Straits Times. (2018), "*Australia passes sweeping anti-encryption legislation*", 6 December, available at: https://www.straitstimes.com/asia/australianz/australian-bid-to-force-tech-firms-to-hand-over-encrypted-data-passes-first-hurdle (accessed 8 April 2019).

Thomson, J.J. (1975), "*The Right to Privacy*", As reprinted in Schoeman, F. (Ed) (1984) Philosophical Dimensions of Privacy, Cambridge: Cambridge University Press.

Tossini, J. V. (2017), "*The Five Eyes – The Intelligence Alliance of the Anglosphere*", available at: https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere, (accessed 5 January 2019)

Turner, M. J. L. (1994), "Case of Vatsal Patel" *Computers and Law, New Series* Vol. 5 No. 1, available at: http://www.computerevidence.co.uk/Cases/Patel/Articles/Patel.htm (accessed 26 September 2019).

UK Government (2016), "*Investigatory Powers Act (IPA)*", available at: http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted (accessed 18 April 2019)

US Department of Justice. (2004), "*Forensic Examination of Digital Evidence: A Guide for Law Enforcement*" available at: https://www.nij.gov/publications/Pages/publication-detail.aspx?ncjnumber=199408 (accessed 5 May 2019).

Vaas, L. (2019), "Five Eyes nations demand access to encrypted messaging", 1 August, available at: https://nakedsecurity.sophos.com/2019/08/01/five-eyes-nations-demand-access-to-encrypted-messaging/ (accessed 24 September 2019).

Van Staden, W. (2013), “Protecting third party privacy in digital forensic investigations”, *IFIP International Conference on Digital Forensics,* pp. 19-31. Springer, Berlin, Heidelberg.

Vanini, U. and Rieg, R. (2019) “Effects of voluntary intellectual capital disclosure for disclosing firms: A structured literature review”, *Journal of Applied Accounting Research*, Vol. 20 No. 3, pp. 349-364.

Voorhees, S. (2017), “Three Mistakes in Responding to Security Incidents, and What To Do Instead”, available at: https://www.infosecurity-magazine.com/opinions/three-mistakes-responding-security/ (accessed 24 September 2019).

Ward, T. (2015), “An English Daubert? Law, Forensic Science and Epistemic Deference”, *The Journal of Philosophy, Science & Law*, Vol. 15 No. 1, pp. 26-36.

Warren, S. and Brandeis, L.D. (1890), “The Right to Privacy”, *Harvard Law Review*, Vol IV No 5, available at: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (accessed 13 April 2019).

Weinberg, B. D. Milne, G. R., Andanova, Y. G. and Hajit, F. M. (2015), “Internet of Things: Convenience vs. privacy and secrecy”, *Business Horizons*, Vol. 58 No. 6, pp. 615 – 624.

Westin, A.F. (1967), *Privacy and Freedom,* New York: Atheneum.

Westin, A.F. (2003), “Social and Political Dimensions of Privacy”, *Journal of Social Issues*, Vol. 59 No. 2, pp. 431-453.

White, G., Lee, A., and Tower, G. (2007), “Drivers of voluntary intellectual capital disclosure in listed biotechnology companies”, *Journal of Intellectual Capital*, Vol. 8 Issue: 3, pp. 517-537.

Whitley, E.A. (2009), “Perceptions of government technology, surveillance and privacy: the UK identity cards scheme”, in Benjamin J. Goold and Daniel Neyland (Eds), *New Directions in Privacy and Surveillance*, pp. 154-177.

Winner, L. (Ed) (1992), *Democracy in a Technological Society, No 9 in the serie Philosophy and Technology*. Boston: Kluwer, Dordrecht.

APPENDIX A: EXPERT REVIEW QUESTIONNAIRE

Expert reviewers were provided with the list of ethical principles in Section 5 and the first draft of the diagram in Section 7 and asked to answer following questions:

1. Is the diagram self-explanatory?
2. Is the diagram understandable?
    a. If not, what is not clear?
    b. How could it be improved?
3. Does the depicted forensics process match your reality in terms of forensics investigations?
4. Please now examine the individual stages. Rank each in terms of:

	Are the components of this stage, as depicted in the diagram, complete? If not, what is missing?	Are the named ethical principles, as depicted in the diagram, appropriate for this stage? If not, which should be removed/added?	In what ways would ethical considerations impact the investigation?
Identification			
Acquisition			
Preservation			
Search			
Analysis			
Reconstruction			
Reporting			

5. Any other comments or suggestions for improvement are very welcome

	USA DoJ (2004)	**Köhn (2013)**	**Casey (2000)**	**DFRWS (2001)**	**Reith (2002)**	**Ciardhuáin (2004)**	**Cohen (2009)**	**Rogers *et al.* (2006)**
IDENTIFICATION	Assessment	Preparation Incident	Recognition	Identification	Identification Preparation	Awareness Authorization Planning Notification	Identification	Planning
ACQUISITION	Acquisition	Incident Response	Preservation Collection Documentation	Preservation Collection	Preservation Collection	Search Identification Collection Transport Storage	Collection Transportation Storage	Triage
SEARCH	Examination	Investigation	Classification Comparison Individualization	Examination	Examination	Examination	Analysis Interpretation	Usage/User Profiles
ANALYSIS								
RECONSTRUCTION (HYPOTHESIS)			Reconstruction	Analysis	Analysis	Hypothesis	Attribution Reconstruction	Timeline
REPORTING & PRESENTATION	Documenting and Reporting	Presentation		Presentation	Presentation	Presentation	Presentation	Case Specific Evidence
PROOF/DEFENSE				Decision		Decision		
REFLECTION & CONCLUSION							Destruction	

Table 8: A Selection of Forensics Investigation Stage Proposals (selected from Ciardhuáin (2004) and Du *et al.* (2017) and augmented)

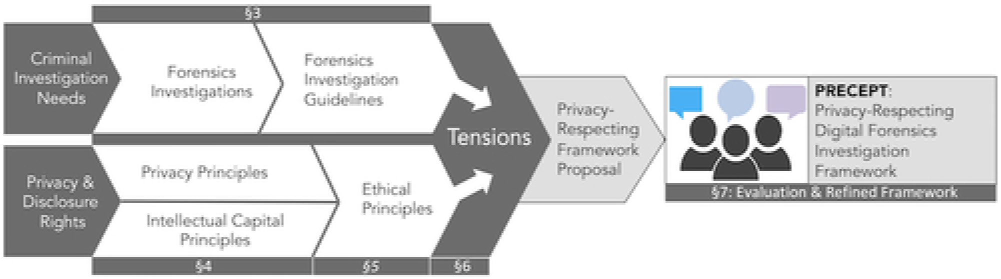
§3
Criminal Investigation Needs
Forensics Investigations
Forensics Investigation Guidelines
Tensions
Privacy & Disclosure Rights
Privacy Principles
Intellectual Capital Principles
Ethical Principles
Privacy-Respecting Framework Proposal
PRECEPT: Privacy-Respecting Digital Forensics Investigation Framework
§7: Evaluation & Refined Framework
§4
§5
§6

Figure 1: The derivation of the ethical framework (Section numbers indicated within the diagram)

84x23mm (150 x 150 DPI)

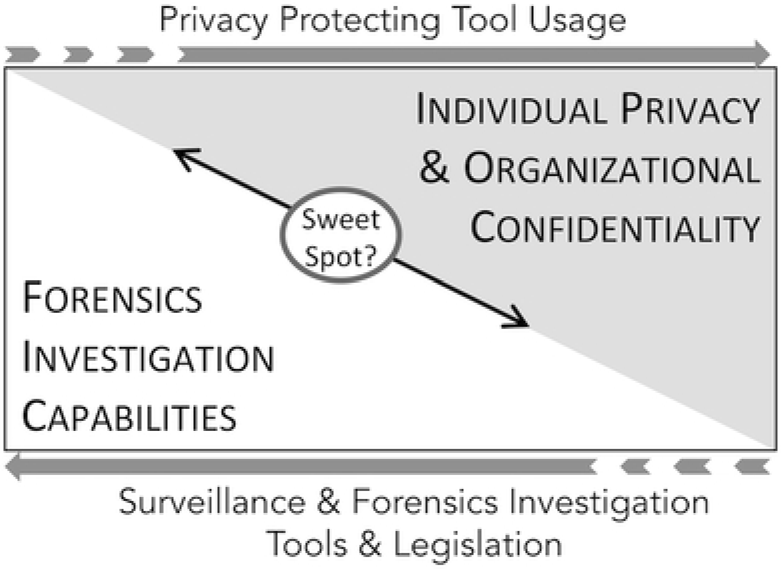
Privacy Protecting Tool Usage
Individual Privacy & Organizational Confidentiality
Sweet Spot?
Forensics Investigation Capabilities
Surveillance & Forensics Investigation Tools & Legislation

Figure 2: The Tension between Privacy & Confidentiality Desires and Rights, and Forensics Investigation Needs and Capabilities

84x49mm (150 x 150 DPI)

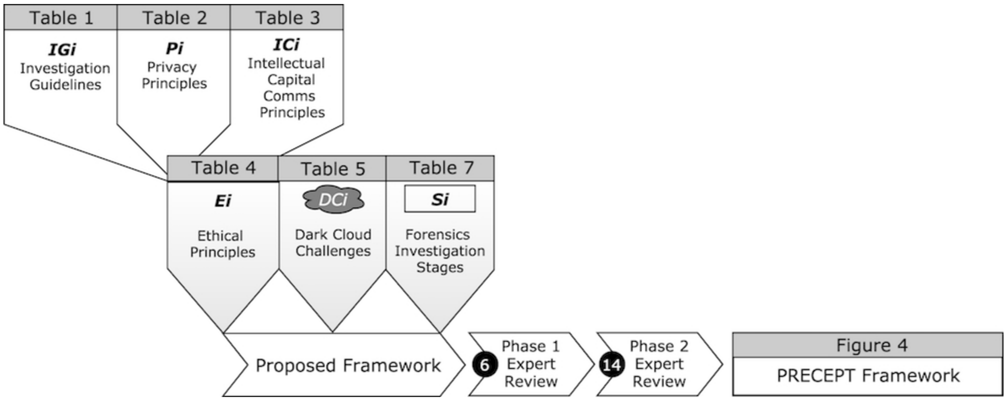

Figure 3: Mapping Privacy Principles (Pi), Intellectual Capital Communications Principles (ICi) and Investigation Guidelines (EGi) to Ethical Principles (Ei), and then aligning these with the stages involved in forensics investigations (Si) and the challenges introduced by the Dark Clouds (DCi), producing the PRECEPT framework.

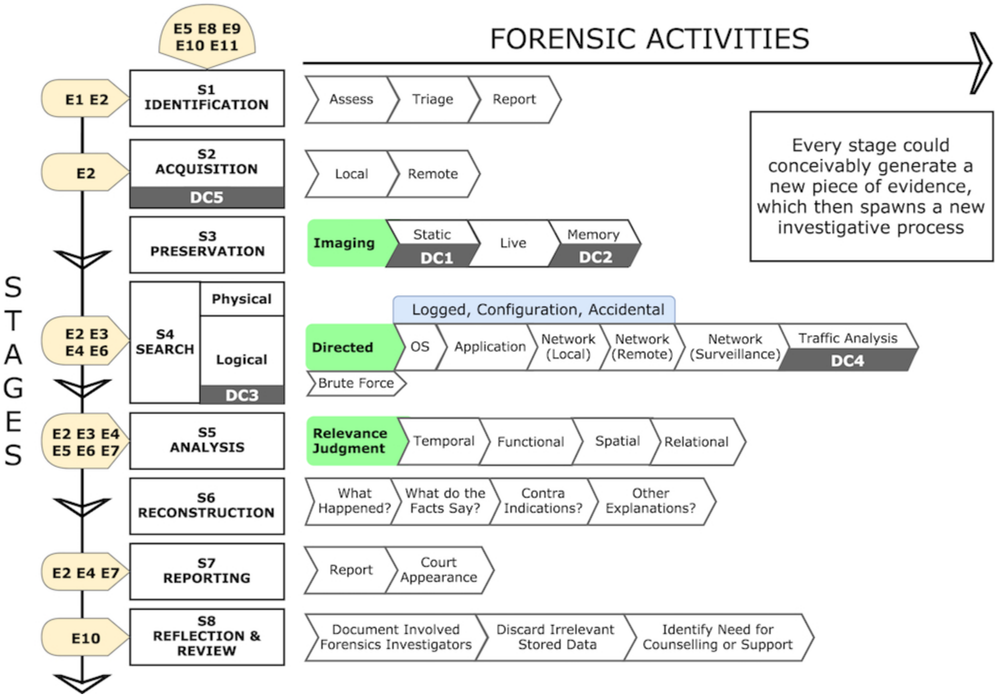

Figure 4: PRECEPT: Privacy-Respecting Forensics Investigation Framework
(Si refers to investigation stages in Table 7, DCi refers to challenges to digital investigations i.e. "Dark Clouds" listed in Table 5; Ei refers to the ethical principles outlined in Table 4).