Legal and Ethical Issues of pre-incident Forensic Analysis

Iain Sutherland[1], Matthew Bovee[2], Konstantinos Xynos[3] and Huw O. L. Read[2]
[1]Noroff University College, Tordenskjoldsgate 9, 4612 Kristiansand S, Norway.
[2]Norwich University, Northfield, VT, USA
[3]Mycenx Consultancy Services, Germany

iain.sutherland@noroff.no
mbovee@norwich.edu
kxynos@mycenx.com
hread@norwich.edu

Abstract: Investigators searching for digital evidence may encounter a variety of different IoT (Internet of Things) devices. Data in such devices and their environments can be both valuable, but also highly volatile. To meet best practices and to process these devices in an expeditious and forensically-sound manner, an investigator should have a predefined plan. Developing such plans requires prior knowledge developed through the exploration and experimentation of the “target” devices. The expanding variety, number, and pervasiveness of IoT devices means there is an increasing need for pre-incident analysis to ensure forensic tools and techniques acquire, preserve and document evidence appropriately. Many of these IoT devices have proprietary file- and operating-systems and may employ mechanisms to protect intellectual property by limiting or preventing access by researchers. Disassembly of the device and circumventing these mechanisms may be restricted by contract, end-user licence agreement (EULA) or legislation regarding intellectual-property rights. Legislative exclusions exist for security research, in some jurisdictions, permitting legitimate analyses. The pre-incident analyses of hardware to establish a forensic process bear some similarity to vulnerability and security research, however there are distinct differences in their end goals. This paper discusses the legal and ethical issues that may be encountered when conducting pre-incident forensics analyses focussing on IoT hardware. It highlights areas of particular concern, identifies best practice and subjects requiring future work as presented in the literature before providing a series of recommendations for forensics investigators processing these types of devices.

Keywords: Forensic practitioners, legal issues, ethical issues, vulnerability research, cyber forensics

1. Introduction: Current challenges

1.1 Challenges of analysis

IoT (Internet of Things) devices provide a variety of monitoring and control functions of personal and environmental factors. The data within these devices can be valuable for the digital investigator, yet highly volatile. Best practice requirements (NIST, 2019; ISO, 27037) demand validation and verification of forensic tools and processes for evidence collection before deployment at a crime scene or use on a device containing potential evidence. Investigators need a clear understanding of the impact of their actions on a device. The continued proliferation of IoT hardware means researchers should be engaged in “pre-incident” research. This can be defined as research focused on exploration of devices prior to an incident to: identify where evidence may be present prior to the device appearing in an investigation; determine how to acquire said evidence; and, document best practice for processing said device. Once an IoT device has been analysed, the results need to be disseminated and verified by others in the community. This verification process ensures that analyses and any proposed methods are correct and helps to identify exceptions, variations, or improvements. Pre-incident research is essential to support practitioners in present and future digital forensics investigations, but may have both ethical and legal implications.

1.2 Prior work

There has been previous work examining the legal and ethical issues of forensics research. Liles et al. (2009) explored the legal issues facing forensics experts which highlighted legal concerns including the interpretation of legislation. Read et al. (2015) focused on the legal and ethical issues of jailbreaking and hardware modification to access devices, and Stoykova et al. (2022) highlighted the legal and technical issues relating to the reverse engineering of file systems. Exploiting vulnerabilities in some cases provides the investigator access to devices that would otherwise be inaccessible. Pessolano et al. (2019) outlined a process for recovering Nintendo 3DS evidence that required use of a flashcart to exploit a vulnerability to access to the device. These flashcarts are advertised for illegally copying games and sale of these devices is now illegal in some jurisdictions. Other similar examples of vulnerabilities used in investigations include checkm8 and checkra1n, used to exploit iOS devices by Cellebrite (Cellebrite, 2020).

In this paper we reiterate that digital forensics best practice requires an established process. Digital investigators therefore are faced with the need to explore a wide range of devices (i.e., using reverse engineering or other similar invasive techniques) as part of pre-incident analyses to expand their understanding of the device. Yet this process is time consuming, technically demanding, and presents legal and ethical challenges that need to be carefully managed.

The rest of this paper is organised as follows; Section 2 identifies the need for pre-incident analysis, Section 3 considers legal and ethical concerns, Section 4 considers the status quo and identifies areas in need of future effort. Finally, Section 5 provides a summary and conclusions.

2. The need for pre-incident analysis

2.1 The requirements of standards and best practice

Forensics researchers and practitioners are guided by standards and codes of best practice, with a key focus on the consistency and reliability of investigative practice and procedures to ensure the admissibility of evidence. These standards are clear on the need for established methodologies and for preparation prior to an incident. ISO/IEC 27037:2012, the international standard, provides guidelines for identification, collection, acquisition and preservation of digital evidence. In section 5.2 it states, "*All processes to be used by the DEFR* [Digital Evidence First Responder] *and DES* [Digital Evidence Specialist] *should have been validated prior to use*" (ISO/IEC 27037:2012). In addition, section 5.3.5 also highlights the importance of justification in handling, obtaining and reproducing digital evidence. It is therefore essential to test and validate a process prior to its use to ensure understanding of the device, and also to share processes and procedures for validation. This is further clarified in ISO/IEC 27041:2016 which outlines the steps required to ensure investigative processes are fit for purpose. This standard defines the way in which requirements can be captured and developed for the design and validation of any new investigative methods. It clearly states that a new method should be accompanied by a validation process with suitable test data.

2.2 Support for IoT Device Examination

Tools to support IoT investigations are limited. Manufacturers may be unwilling to provide device or data access, citing privacy or intellectual property concerns (SWGDE, 2022). A high-profile example that received much public attention and interest is Apple's reluctance to provide access to the contents of an iPhone in the Apple V FBI encryption case (United States District Court, 2016). A further challenge is that device types may also undergo rapid updates, so manufacturers might be *unable* to produce a duplicate device if the case in question involves an older or obsolete model. In addition, the device may have undocumented behaviour as a result of a vulnerability or modification. If manufacturers provide a new device this may exhibit different behaviour from an older evidentiary device that has been patched, updated and contains user data. Activities needed to aid understanding of a device may, in some cases, include the need to access and dump proprietary code for analysis (Dawson and Akinbi 2021). The limited support at present means that there may be the need to reverse engineer firmware to understand the operation of the device or to extract encryption keys to decrypt information held in the device (Pessolano et al. 2019).

2.3 Supporting Digital Forensics Practitioners

Device capabilities also need to be understood to support appropriate triage-process decision-making. Frameworks for IoT readiness and knowledge of IoT systems are highlighted as key areas for forensic readiness (Zulkippli et al., 2021). There is a need to understand the devices and systems if we are to address the types of problems mentioned by Luciano et al., (2018); there exists a

> *"... lack of funding towards research, training and forensic tools in IoT and these should be one of the most important research opportunities in the future ..."*

Horsman (2019) outlined that the pressures on the forensic practitioner are such that they may need to rely on the publication of forensic research to develop processes and procedures. There is a developing body of work exploring the expanding range of consumer devices to determine if the information left on systems might be of value to a forensic investigation and how to access this in a forensically sound manner. Examples include games systems (Barr-Smith et al., 2021), home routers (Awasthi et al., 2018), smart TV's (Sutherland et al., 2014; Boztas et al., 2015) and robot vacuum cleaners (Zhou et al., 2022). Grouping such devices together under the banner of IoT is challenging due to varying levels of interactivity and security, copy protection mechanisms, and disparate types of evidence. Some work may even be funded by government research (e.g. Barr-Smith et al., 2021). However, researchers who share guidance in the forensic community to support investigations could come into conflict with manufacturers seeking to protect user data and intellectual property.

3. Legal and Ethical concerns

3.1 Legal issues

The focus on legal aspects of forensics research has been on examination and preservation of the evidence chain and on requirements of expert witness work (e.g. Huang, 2021). There appears to be a lack of discussion on the challenges surrounding the pre-incident analysis of systems as part of forensic readiness. Gamero-Garrido et al., (2017) examined the legal risks of third-party vulnerability research, noting it is possible to seek permission to carry out an analysis, but response rates varied between 20% and 40%. The work also noted 22% of security researchers polled had received legal threats due to their vulnerability research. It would be of interest to the digital forensics community to identify if there are similar issues when considering research supporting law enforcement, as is the focus of pre-incident analysis.

Beyond the "do" and "don't" approaches taken in End User Licence Agreements (EULAs), there are significant legal and best-practice documents that cover permissibility of security/vulnerability research. Table 1 presents several from the context of digital forensics research. Such legal protections broadly encompass pre-incident work to facilitate forensics on behalf of the legal system. Certain jurisdictions expressly exempt investigation action in support of law enforcement when backed by a court order. This would include forensics, although possibly only pursuant to an active case. Some jurisdictions allow for work in the "public interest", while other definitions of "good faith security research" do not appear to encompass digital forensics research, being more focussed on vulnerability and cyber security research aimed at protecting specific systems.

In some jurisdictions, such as the UK, there is no statutory defence for legitimate security research. As outlined in Table 1 the Crown Prosecution Service guidance (Crown Prosecution Service, 2020) states that various factors must be considered to determine if the prosecution is in the public interest, for instance; financial gain, concealment of identity and in particular how any tools or 'articles' created by the work have been used. The guidance states*; "For example, whether the article was circulated to a closed and vetted list of IT security professionals or was posted openly."* (Crown Prosecution Service, 2020) which has significant implications on the way that tools developed by academics as part of pre-incident research might be published, the how results of a pre-incident analysis can be validated, and whether any tools and datasets developed can be shared.

Table 1. Key Details of Example Pertinent Laws, Regulations, Acts, and Guidance.

Digital Millennium Copyright Act (1986)	Allows lawfully authorised investigative, protective, information security, or intelligence activity by officers, agents, or employees of the United States, a State, or a political subdivision of a State, or a person contracted by them. Other individuals are limited to a definition of "security testing" that does not appear to include research to identify forensically-sound means of identifying and acquiring evidence.
Computer Misuse Act (1990)	UK legislation with penalties of imprisonment and fines for any attempt (whether successful or even possible) to secure or facilitate unauthorised access to data. Although Crown Prosecution Service (2020) CMA Prosecution Guidance states where CMA violations are performed in the "public interest", prosecutors are advised to consider financial, reputational, or commercial damage caused to victims, and whether the purpose of the offence was for financial gain.
Computer Fraud and Abuse Act Charging Policy Guidelines (2022)	Prosecution should be declined if a defendant's conduct and intent was that of "good-faith security research". Such research is, however, narrowly defined in such a way that it does not appear to include digital forensics.
Electronic Frontiers Foundation (2021)	Electronic Frontier Foundation (EFF) Coders' Rights Project Vulnerability Reporting FAQ that provides guidance that focuses primarily on vulnerability research, but many of the recommendations and advisements apply to digital forensics, such as: seeking legal advice in advance; publishing only non-functional/non-code details/results; being aware of the impacts of copyright and trade-secret laws
Extraction of Information from electronic devices: code of practice, UK Home Office	Guidance refers to the Data Protection Act (DPA) and the General Data Protection Regulation (GDPR), both of which focus on protecting the data of

(Home Office 2022)	individual persons.
Council of Europe, Convention on Cybercrime,(2001)	Council of Europe, Convention on Cybercrime, European Treaty Series – No. 185 recommends each signatory adopt legislation and other measures to criminalise intentional unauthorised access to any or all of a computer system, or making available a “device” to aid such access.
Computer Fraud and Abuse Act (CFAA) (1986).	Sets a test value of USD 5,000 damage due to unauthorised access to any protected computer in any one-year period, and provides for imprisonment of up to five years

Guidance in relation to prosecution under the US Computer Fraud and Abuse Act (Computer Fraud and Abuse Act Charging Policy Guidelines, 2022) included good faith security research for the first time in 2022. The phrase ‘investigation’ is cited as a valid reason for research, but this is then followed with a statement that the primary goal of such work should be to improve the safety and security of the device, the services it supports, or the related users (Computer Fraud and Abuse Act Charging Policy Guidelines (2022). This appears not to include pre-incident analysis in support of a forensic investigation as a valid reason. Even if that *was* intended, there is nothing to preclude a vendor that believed it had been harmed by such investigative actions from filing suit and leaving it to the courts to evaluate the guidance.

3.2 Ethical issues

Pre-incident analysis also raises some issues from an ethics perspective. While various codes of ethics exist (Table 2), there is no unified code of ethics for digital forensics. The need for a code of ethics for digital investigations was highlighted by Seigfried-Spellar et al., (2017), and work such as that conducted by Horsman (2022) has explored the ethical issues and concerns from the privacy perspective and the impact of an investigation on the individual. Ferguson et al. (2020) in their paper highlight the ethical issues of an investigation on both individual privacy and organisational confidentiality. The issue of disclosing organisational intellectual capital / intellectual property is addressed, with the observation that forensics investigations have the possibility to disclose intellectual capital and therefore cause damage to an organisation.

A comparison of ethics for different professional organisations is presented in Table 2. Codes of practice, of ethics, and mixed aspects of both exist, but do little to resolve tension between the need for pre-incident examination, preparation and various legal constraints. Some codes say to act legally or the equivalent, while simultaneously exhorting activities (e.g., training, experience, validation of methodology) that benefit from pre-investigative research and preparation. The need, however, is to have broader documented exemptions and protections for work completed ethically that ultimately benefits the courts, Law Enforcement Agency (LEA) agencies, the legal system, their related processes and the community as a whole.

Table 2: Example Code Details from Select Organisations.

ACM Ethics (2023)	Section 2.3 states “Know and respect existing rules pertaining to professional work. where "Rules" here include local, regional, national, and international laws and regulations.
Digital Forensics Certification Board (DFCB) (2003)	Under “Professional Care and Competence”: understand the nature and scope of work presented; be competent and accept engagements within one’s scope of competence; and, utilise validated/appropriate methods, techniques, standards, and controls.
IEEE Code of Ethics (2003)	Improve the understanding by individuals and society of the capabilities and societal implications of conventional and emerging technologies; avoid unlawful conduct in professional activities; maintain and improve technical competence; undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations; and, avoid injuring the property of others
International Association of Computer Investigative Specialists (IACIS) (2019)	Advise/assist within the scope of one’s “legal authority”; be honest and ethical *when dealing with each other*
International Society of Forensic Computer Examiners (2009)	Never reveal anything confidential without a competent court order or express permission by the client, engage in any unethical or illegal conduct, or knowingly undertake an assignment beyond one’s skills
(ISC)^2 (2023)	Act honourably, honestly, justly, responsibly, and legally (including observing all contracts and agreements, express or implied). Simultaneously, provide diligent and competent service to principals, and advance and protect the profession.

3.3 Legal and Ethical issues: A comparison to Vulnerability Research

The current ethical guidance and statutory defences present in legislation are focussed on narrowly-defined legitimate cyber security research, and typically relate to vulnerability analysis. Vulnerability research is concerned with determining if security measures can be circumvented due to errors in the device's design or functionality. However, forensics is concerned with the information available in the device, and the accuracy of methods used to extract data. To be forensically useful, extractions should be repeatable, each iteration providing exact copies of the data held in the device.

In pre-incident research a vulnerability may be used as a step in the process. Video-game hacking, on which some forensics methods rely (Pessolano et al., 2019) shares similarities to vulnerability researchers, searching for issues in software and hardware, but as a means to obtain additional access to a games system. Device manufacturers apply various methods and techniques, like cryptography and obfuscation, as a defence mechanism to keep the system and its contents hidden from those wanting to engage in hacking/reverse-engineering of copy-protection mechanisms. The research performed on these proprietary systems is not dissimilar to "Blackbox" analysis. This requires extensive knowledge, experience and specialist tools, but has been known to generate results containing misunderstandings, errors and even omissions during the reverse engineering process. A digital forensic analyst relying on research from such groups must be wary of the temporal nature that afflicts these communities. Websites hosting information may disappear without notice, resellers of hardware that can circumvent security may go out of business (or may be removed because of legal proceedings), toolsets may not be updated and malfunction on newer versions of devices. All these issues create uncertainty and an almost ephemeral nature to digital forensic capability.

Responsible vulnerability research has a defined best practice of disclosing the issue to the manufacturers to enable a corrective action, a patch to be developed, before the vulnerability is disclosed to the wider community. Ideally in a pre-incident analysis to ensure the validation, it is the process, methods and tools developed that should be disseminated for validation. Horsman (2019) summarised the key attributes of an digital artefact that should be communicated for research to be of value to the forensics community including: the full details of the artefact; any methodology used; and, appropriate test data. The manufacturer is not involved in this process. Currently there are different approaches to this dissemination with some entities providing data for wider analysis (VTO Labs, 2023) and some such at the Artefact Gnome Project (Artefact Gnome Project, 2023) being more restricted.

In some cases pre-incident research may be a breach of the terms and conditions, and involve processes that may conflict with ethical codes of practice. It may also skirt close to what is permitted by national laws. Care must be taken to avoid publishing material that may be seen as promoting breach of copyright or the disclosure or theft of intellectual property.

4. Discussion and areas for future work

4.1 The need for legal clarification

Local legislation needs to address the issue of limitations introduced when making reverse engineering acts illegal. It is unclear what happens when law enforcement needs or relies on work products potentially deemed illegal or impermissible by local legislation. Legislation could also address concerns over manufacturers providing access to devices to circumvent encryption / privacy mechanisms. This is still a current concern for law enforcement (Wray, 2021).

Differences in legal and ethical frameworks could hamper forensics research in certain areas or jurisdictions, leading to an overreliance on material produced in *other* jurisdictions and loss of local capability. A valid concern for technology companies and lawmakers in changing legislation or in allowing further exemptions (such as those applied to the DMCA in the USA) would be the risk of accidentally permitting research that exposes intellectual property under the guise of valid forensics research. This would require some degree of regulation.

4.2 Clarification of codes of ethics

While there are numerous examples of codes of ethics, they have the challenge of addressing the tension between the absolute, strict interpretation of the legal constraints, the due diligence requirements of many codes of ethics/best-practice and of digital evidence examiner professions, the evidential needs of the legal system, and LEA and examiner resource limitations. It is clear that pre-incident analysis will require a strong set of ethical statements. Standard operating procedures and clear Code of Ethics are essential to define best practice and avoid unethical behaviour in this type of research. The authors would recommend one that is concise. The IEEE Code of Ethics (2023) provides a good example of such an attempt. We present three headings:

- To uphold the highest standards of integrity, responsible behaviour, and ethical conduct in professional activities.
- To treat all persons fairly and with respect, to avoid harassment or discrimination, and to avoid injuring others.
- To strive to ensure this code is upheld by colleagues and co-workers.

These provide appropriate high-level principles. In addition, the best practice guidance in Table 3 should be considered.

Table 3: Best Practices, also drawing on vulnerability research recommendations from the Electronic Frontiers Foundation (Electronic Frontiers Foundation, 2021).

Legal Process	**Legal within the jurisdiction** While a basic requirement, this is highlighted in *The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research* (Bailey, 2012) as a specific concern as *compliance* with the laws in that jurisdiction is seen as critically important.
Logical Device Selection	**The selection of the target of the pre-incident investigation should be described, appropriate and based on potential evidential value.** Any examination of a device should have a rational methodology for device selection based on type, availability, cost, potential evidence etc. The selection rationale should be open and clearly described.
Owned Device	**All experimentation should take place on a device purchased for the purpose.** Second-hand devices should be avoided (or blindly sourced) to avoid targeted recovery of personal data. If there is a risk of personal data being recovered then appropriate institutional ethical review may be needed.
Focused Analysis	**Although examination of a device might expose Intellectual Property, the analysis and results should focus on evidence sources and user activity / interaction. This should avoid proprietary areas / information where possible.** This should be focussed on potential evidence. This is usually user activity / settings / usage of the device etc. Care should be taken to protect Intellectual Property (IP) and not provide tools or techniques that access/expose areas of the device without need.
Limited Dissemination	**While peer reviewed publication is prevalent, and there is a shift for open access to all datasets and tools, for pre-incident analysis this should only be supplied to LE or other researchers for validation / verification and peer review.** The scientific approach requires verification / validation by other researchers. Dissemination should be limited to ensure access to tools and datasets only for validation / verification of the method, further research, and law enforcement use. Wider dissemination should be limited, if it would cause harm to the industry. Therefore, researchers would need to apply some mechanism to decide on the benefit to society.

Proactive forensics research needs to be done with care to ensure legal and ethical considerations are taken into account when deciding to examine a device. The permitted activities can depend very much on the jurisdiction in which the device is being examined. This can be an added complexity if the research team is international and spanning several different jurisdictions. One way to address ethical considerations may be to expand the oversight of Research Ethics Committees (RECs) (Europe) and Institutional Review Boards (IRB) (in the USA) which usually are focused on potential harm to the individual and attentive to personal rights as espoused in the Belmont Principles which address respect for persons, beneficence and justice (fairness and equality). These committees or boards could assess similar ethical considerations with regard to research, research processes and their results.

5. Summary and conclusion

International standards and best practice guidelines define the requirement for tested, verified methods for the forensic analysis of IoT devices. There is clearly a current and increasing need for forensics research to explore IoT devices prior to an incident occurring, to determine if information of evidential value is present, and to develop best practice for accessing and extracting that information. This forensic intelligence analysis clearly aligns with practices seen in the numerous on-going papers by researchers exploring devices. Labs and forensic practitioners need access to the research in published work (i.e., academic or blogs), but should also be able to access datasets to verify and better understand the processes presented.

There is a demonstrable need for pre-incident analysis, but also a clear tension with current legislation in some jurisdictions. Security and vulnerability research is already very familiar with this tension, although exemptions and codes of practice for prosecutors recognise the value of security-related research. The question remains whether ongoing work with pre-incident analysis falls into this category by design, by accident, or at all as some legislation clearly emphasises that the work is only permitted for the identification and reporting of security vulnerabilities. There is a reliance on the current interpretation of procedural practice continuing to recognise the value of on-going forensic work. Perhaps the root of the issue, at least in the UK and USA, is that computing legislation is over 30 years old and technology and the associated law enforcement challenges have moved on considerably since this legislation was enacted. It is recognised that prosecution procedural practises are regularly updated, but this still poses a challenge, highlighted in the UK by the current campaign for a statutory defence for responsible security research to be enshrined in law (CyberUp, 2022).

In terms of ethical codes there is also a disparity between the need for pre-incident research on the phrasing of some current ethical codes. In this paper, current legal, ethical, and best practice for pre-incident digital forensics research has been discussed, and found to be lacking when compared to the more-established areas of vulnerability research. Opportunities for further work in the harmonisation between these two related areas, particularly in legal and ethical guidance is needed to ensure digital forensic capability is maintained in the future.

6. References

ACM Ethics (2023), ACM Code of Ethics and Professional Conduct, [Online] https://ethics.acm.org/

Artifact Gnome Project (2023) https://agp.newhaven.edu/about/start/

Awasthi, A.; Read, H.O.; Xynos, K.; Sutherland, I. (2018) Welcome pwn: Almond smart home hub forensics. Digital Investigation. 2018, 26, 38–46.

Bailey M., Dittrich D., Kenneally E., Maughan D. (2012) The Menlo Report. IEEE Security and Privacy Volume 10 Issue 2 March 2012 pp 71–75 https://doi.org/10.1109/MSP.2012.52

Barr-Smith F., Farrant T., Leonard-Lagarde B., Rigby D., Rigby S., Sibley-Calder F. (2021) Dead Man's Switch: Forensic Autopsy of the Nintendo Switch. Forensic Science International: Digital Investigation, Volume 36, Supplement, April 2021, 301110. https://doi.org/10.1016/j.fsidi.2021.301110

Boztas A, Riethoven A.R.J Roeloffs M. (2015) Smart TV forensics: Digital traces on televisions, Digital Investigation, Volume 12, Supplement 1, 2015,Pages S72-S80,ISSN 1742-2876, https://doi.org/10.1016/j.diin.2015.01.012

Cellebrite (2020) A Practical Guide to checkm8 – Cellebrite UFED. [Online] https://cellebrite.com/en/a-practical-guide-to-checkm8/

Computer Fraud and Abuse Act (CFAA) (1986). [Online] https://www.congress.gov/bill/99th-congress/house-bill/4718

Computer Misuse Act (1990) [Online] https://www.legislation.gov.uk/ukpga/1990/18

Computer Fraud and Abuse Act Charging Policy Guidelines (2022) [Online]
https://www.justice.gov/jm/jm-9-48000-computer-fraud

Crown Prosecution Service (2020) Computer Misuse Act: prosecution guidance. [Online] https://www.cps.gov.uk/legal-guidance/computer-misuse-act

Council of Europe, Convention on Cybercrime,(2001) European Treaty Series – No. 185. (2001) [Online] https://rm.coe.int/1680081561

CyberUp (2022) Legitimate cyber security activities in the 21st century: Assessing the current consensus of what should constitute legitimate cyber security activity under a reformed UK Computer Misuse Act 1990. [Online] https://www.cyberupcampaign.com/s/CyberUp-campaign-V3-2022.pdf

Dawson, L., Akinbi, A., (2021) Challenges and opportunities for wearable IoT forensics: TomTom Spark 3 as a case study,
Forensic Science International: Reports, Volume 3, 2021, 100198, ISSN 2665-9107, https://doi.org/10.1016/j.fsir.2021.100198.

Digital MIllennium Copyright Act (1998) [Online]
https://www.copyright.gov/dmca/

Digital Forensics Certification Board (2003) Code of Ethics and Standards of Professional Conduct. [Online] https://dfcb.org/code-of-ethics-and-standards-of-professional-conduct/

Electronic Frontiers Foundation (2021) Coders' Rights Project Vulnerability Reporting FAQ [Online] https://www.eff.org/issues/coders/vulnerability-reporting-faq

Ferguson, R.I., Renaud, K., Wilford, S. and Irons, A. (2020), "PRECEPT: a framework for ethical digital forensics investigations", Journal of Intellectual Capital, Vol. 21 No. 2, pp. 257-290. https://doi.org/10.1108/JIC-05-2019-0097

Gamero-Garrido A., Savage S., Levchenko K., Snoeren A. C. (2017) Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research. CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security October 2017 Pages 1501–1513 https://doi.org/10.1145/3133956.3134047

Home Office (2022) Extraction of Information from electronic devices: code of practice [Online] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1110883/E02802691_Electronic_Devices_Code_of_Practice_WEB.pdf

Horsman, G. (2019) Raiders of the lost artefacts: Championing the need for digital forensics research,
Forensic Science International: Reports, Volume 1, 2019, 100003, ISSN 2665-9107, https://doi.org/10.1016/j.fsir.2019.100003.

Horsman, G. (2022) Defining principles for preserving privacy in digital forensic examinations, Forensic Science International: Digital Investigation, Volume 40, 2022, 301350, ISSN 2666-2817, https://doi.org/10.1016/j.fsidi.2022.301350.

Huang J., (2021) When Digital Forensic Research Meets Laws, 2012, 32nd International Conference on Distributed Computing Systems Workshops. https://doi.org/10.1109/ICDCSW.2012.45

IEEE Code of Ethics (2023) [Online] https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/corporate/ieee-code-of-ethics.pdf

International Association of Computer Investigative Specialists (2019) IACIS Code of Ethics and Professional Conduct. [Online] https://www.iacis.com/wp-content/uploads/2019/11/IACIS-Code-of-Ethics-and-Professional-Conduct-Ver-1.4.pdf

International Society of Forensic Computer Examiners (2009) Code of Ethics and Professional Responsibility, [Online] https://www.certified-computer-examiner.com/ethics2.htm

(ISC)² (2023) Code Of Ethics [Online] https://www.isc2.org/ethics/

ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. [Online] https://www.iso.org/standard/44381.html

ISO/IEC 27041:2015 - Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method. [Online] https://www.iso.org/standard/44405.html

Liles, S., Rogers, M., Hoebich, M. (2009). A Survey of the Legal Issues Facing Digital Forensic Experts. In: Peterson, G., Shenoi, S. (eds) Advances in Digital Forensics V. Digital Forensics 2009. IFIP Advances in Information and Communication Technology, vol 306. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-04155-6_20

Luciano L., Baggili I., Topor M., Casey P., Britinger F., (2018) Digital Forensics in the Next Five Years. ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security August 2018 Article No.: 46 Pages 1–14 https://doi.org/10.1145/3230833.3232813

NIST (2019) Computer Forensics Tool Testing Program (CFTT) [Online] https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

Pessolano G., Read H.O.L., Sutherland I., Xynos K., (2019) Forensic Analysis of the Nintendo 3DS NAND, DFRWS-USA July 14-17 Portland, Oregon, USA in Digital Investigation: The International Journal of Digital Forensics & Incident ResponseVolume 29 Issue S Jul 2019 pp S61–S706 https://doi.org/10.1016/j.diin.2019.04.015

Read H., Sutherland I., Xynos K. and Roarson F., (2015), Locking out the Investigator: The need to circumvent security in embedded systems., Information Security Journal: A Global Perspective, vol24. Issues 1-3, 2015. Pages 1-9, http://dx.doi.org/10.1080/19393555.2014.998847

Seigfried-Spellar, Kathryn C.; Rogers, Marcus; and Crimmins, Danielle M.,(2017) "Development of A Professional Code of Ethics in Digital Forensics" (2017). Annual ADFSL Conference on Digital Forensics, Security and Law. 12.

Stoykova, R., Nordvik,R., Ahmed, M., Franke, K., Axelsson, S., Toolan,F., (2022) Legal and technical questions of file system reverse engineering,Computer Law & Security Review, Volume 46, 2022, 105725, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2022.105725

Sutherland I., Xynos, K., Read, H., Jones, A., Drange T., (2014) A forensic overview of the LG Smart TV, presented at the 12th Australian Digital Forensics Conference 2014 SRI Security Congress, "Security on the Move" 1-3 December, 2014, Perth, Western Australia.

Scientific Working Group on Digital Evidence SWGDE (2022) Best Practices for On-Scene Identification, Seizure, and Preservation of Internet of Things (IoT) Devices (2022)

United States District Court (2016) In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, Case No. 15-0451M. [Online] https://www.documentcloud.org/documents/2722199-5-15-MJ-00451-SP-USA-v-Black-Lexus-IS300.html

VTO Labs(2023) IoT Forensics [Online] https://www.vtolabs.com/iot-forensics

Wray C.A. (2021) Statement of Christopher A. Wray Director Federal Bureau of Investigation before the Committee on the Judiciary United States Senate, at a hearing entitled “Oversight Of The Federal Bureau Of Investigation: The January 6th Insurrection, Domestic Terrorism, And Other Threats” Presented March 2, 2021. [Online] https://www.justice.gov/file/1525301/download

Zhou, H., Deng, L., Xu, W., Yu, W., Dehlinger J., and Chakraborty S., "Towards Internet of Things (IoT) Forensics Analysis on Intelligent Robot Vacuum Systems," *2022 IEEE/ACIS 20th International Conference on Software Engineering Research, Management and Applications (SERA)*, Las Vegas, NV, USA, 2022, pp. 91-98, https://doi.org/10.1109/SERA54885.2022.9806735

Zulkipli N.H.N., Willis G.B. (2021) An Exploratory Study on Readiness Framework in IoT Forensics Procedia Computer Science Volume 179, 2021, Pages 966-973 https://doi.org/10.1016/j.procs.2021.01.086