The Effects of Legal Guidelines and Issues of Privacy on Digital Forensics in the United States

Hans L. Peterson

Department of Cybersecurity, Old Dominion University

IDS 300W: Interdisciplinary Theory & Concepts

Dr. Kat LaFever

November 23, 2024

Abstract

Legal guidelines and privacy issues dictate digital forensics in various ways. This study investigates how legal guidelines and issues of privacy affect the development of digital forensic tools, procedures, and standards for digital forensic investigations. Using interdisciplinary techniques, this study combines insights from the disciplines of law, computer science, and criminology to produce a comprehensive understanding. After conducting a literature review, research reveals guidelines, such as the Daubert Standard and Federal Rules of Evidence, determine the handling of digital evidence. Additionally, the modifiable nature of digital evidence and the usage of revolutionary software to collect digital evidence present admissibility issues in court. Lastly, a lack of nationwide standardization and credentialing for digital forensic professionals increases the risk of rendering evidence inadmissible. As a result, legal guidelines and issues of privacy mainly dictate the practices, certification, and tools under digital forensics.

Keywords: digital forensics, digital evidence, Daubert Standard, legal guidelines, privacy.

The Effects of Legal Guidelines and Issues of Privacy on Digital Forensics in the United States

Introduction

In the modern era, the expanse of technology has led to breakthroughs in digital forensic tools. However, the advent of revolutionary technologies, such as artificial intelligence and IoT devices, has posed many legal and privacy issues in digital forensics. The concerns for privacy and the development of legal guidelines have shaped the field of digital forensics as a result. What are the effects of legal guidelines and issues of privacy on digital forensics in the United States then? This study uses the insights from the disciplines of law, criminology, and computer science to examine these effects.

Law is used in this study since it examines the issue of privacy in the development of policies and laws guiding digital forensic procedures. Criminology focuses on the standardization of procedures in digital forensic investigations. Computer science studies possible limitations on digital forensic tool usage in investigations. Using an interdisciplinary approach helps accomplish a comprehensive understanding of the effects, which can better inform future practices for digital forensics. Digital forensics is ever-evolving, and so is technology, law, and crime. Change is constant, so we must adapt. As for cybersecurity analysts, they must be aware that they operate on rules and procedures, just as digital forensic analysts work within jurisdictions and use certain technologies in investigations. It is crucial to know why certain laws and procedures exist so that one understands the value of obeying them.

Key Terms

Daubert Standard, digital forensics, privacy, and admissibility are key terms in this study. Manes, a doctor of computer science from the University of Tulsa, and Downing (2009) define the *Daubert Standard* as the requirement for all evidence to be relevant, reliable, empirically testable, peer reviewed, and acquired through techniques acceptable to the relevant scientific community. Essentially, the *Daubert Standard* tests the admissibility of evidence presented by expert testimony. Vincze (2016), a director of a Crime Investigation graduate program at George Washington University, defines *digital forensics* as the use of proven methods to collect, validate, and analyze digital evidence from digital devices to assist with reconstructing events deemed criminal. Dehghantanha, a graduate of computer science, and Franke (2014) define *privacy* as "the right to control who knows certain aspects about you, your communication, and your activities." Ryan, a lawyer and adjunct professor of George Washington University, and Shpantzer (2002) define *admissibility* as evidence being "relevant, material, and competent, and its probative value must outweigh any prejudicial effect."

Law

Like other fields of forensic sciences, the method of collection, analysis, and validation of digital evidence is scrutinized; evidence, digital and physical, must be admissible in court. Evidence must survive the Daubert test, which is now known as the Daubert Standard (Ryan & Shpantzer, 2002). However, since digital evidence can be easily modified without leaving traces, there are issues with its competency in court (Ryan & Shpantzer, 2002). Digital forensics is a relatively new discipline that lacks the standardization that older disciplines have. Because of the lack of standardization, the methods used to collect digital evidence are questioned. Furthermore,

the usage of innovative digital forensic tools may threaten an evidence's admissibility in court (Adams, 2008). Since these tools are newer and less used than the industry standard, they are less accepted in the scientific community. Breakthroughs in digital forensic tools must adhere to legal guidelines while simultaneously advancing techniques.

Criminology

In forensic science, it is vital to collect evidence during investigations. For digital forensics, these investigations are further complicated because analysts must follow the investigatory scope and protect their target's privacy. Investigators must plan investigations ahead to minimize breaches of privacy while seizing data, but the methods of doing so depend on the agency (Vincze, 2016). For an individual to protect their privacy from investigation, devices should be encrypted. However, cybercriminals also adopted this strategy to hide their criminal activity, ultimately creating inaccessible devices (Vincze, 2016). As a result, many devices obtained in investigations are never processed. Furthermore, it is necessary to develop a standardized system to certify digital forensic professionals to prevent digital forensics from being discredited as a scientific discipline (Zahadat, 2019). If digital forensics is discredited, then the analyzed digital evidence lacks reliability and admissibility. Certification, investigatory procedures, and the peer review process need to be standardized to ensure evidence is admissible.

Computer Science

While the Daubert Standard is widely adopted across the states, not every state uses it as a guideline for handling evidence. Major guidelines, such as the Federal Rules of Evidence (FRE) and case law, can also dictate how evidence is handled (Manes & Downing, 2009).

Practitioners use industry-standard tools and techniques to fulfill FRE requirements, and they maintain the chain of custody for evidence (Manes & Downing, 2009). However, the main issue lies mostly in the expert testimony, where, like the Daubert Standard, the techniques used to obtain digital evidence are scrutinized. As for case laws, they can set precedents on an evidence's admissibility. Furthermore, privacy regulations in the US rely more on industry self-regulations (Dehghantanha & Franke, 2014). For example, the PCI-DSS regulates security for credit card handling. Despite privacy regulations and laws, certain acts can override such restrictions. The USA-Patriot Act allows analysts to collect digital evidence without privacy limitations if the analysts suspect that the target is involved in terrorism (Dehghantanha & Franke, 2014). Essentially, analysts can bypass the scope of an investigation.

Common Ground

There are three commonalities between the three disciplines. First, computer science and law show how guidelines determine the handling of evidence. For example, computer science and law reveal the guidelines, such as the Daubert Standard and FRE, that practitioners must be aware of to preserve evidence's admissibility (Manes & Downing, 2009; Ryan & Shpantzer, 2002). Second, criminology and law emphasize a necessity to standardize digital forensics nationally. Criminology focuses mainly on the certification of digital forensic professionals, while law focuses on the importance of using industry-standard tools (Zahadat, 2019; Adams, 2008). Third, criminology and computer science find privacy to be a main concern. Criminology reveals the planning of investigations to minimize privacy violations, and computer science details the US's reliance on self-industry regulations for privacy (Vinzce, 2016; Dehghantanha & Franke, 2014). Without interdisciplinary research, these commonalities would not be found since only one discipline would be referred to. For example, the computer science perspective might

falsely be assumed to be only concerned with digital forensic tools when, in reality, it also emphasizes the importance of following guidelines when investigators collect evidence.

Disciplinary Conflicts

Two of the conflicts between insights are standardization and privacy. In the context of preserving admissibility, criminology pushes for revolutionary changes to digital forensics by standardizing procedures, tools, and certification nationwide; a disciplinary finding in law, however, only emphasizes usage of industry-standard tools for all practitioners. Regarding privacy, a disciplinary finding in computer science conflicts with other insights in the same discipline and criminology. Under the USA-Patriot Act, practitioners can overstep investigatory scopes and limits on privacy based on suspicions of terrorism; other findings in computer science and criminology emphasize the minimization of breaching privacy.

Criminology and law stress standardization differently. Despite standardization meaning that something conforms to a baseline, that baseline acts more so as a spectrum based on location. While national standards for digital forensic practices should exist, exceptions and deviations should be allowed to ensure these practices align with a state's requirements. Like standardization, computer science and criminology emphasize privacy differently. Although privacy can be understood as the right to control what a person may know about you, the right may be disregarded in scenarios where you pose a grievous threat to other individuals. Due to the high sensitivity of investigations under the USA-Patriot Act, they require a different, more cautious set of procedures compared to ordinary digital forensic investigations. The right to privacy differs based on a target's intent to harm others.

Ch. 12: "Constructing a More Comprehensive Understanding or Theory"?

Overall, legal guidelines and issues regarding privacy dictate digital forensics; specifically, they dictate procedures, tools, and the authority of investigators. There are four main causes that, combined together, hinder developments in digital forensics: guidelines for handling evidence, the right for an individual to have privacy, the concept of admissibility, and the lack of standardization. Guidelines, such as the Federal Rules of Evidence, restrict investigatory scopes and digital forensic procedures. Brought by the 4th amendment of the U.S. Constitution, individuals have a right to privacy. Investigators must respect these boundaries during investigations, even when attempting to access encrypted devices. Moreover, admissibility is a requirement for evidence to be admitted in court. If the evidence does not pass the Daubert Standard, such as when investigators use revolutionary tools not accepted by the digital forensic community, it becomes inadmissible. Lastly, the lack of standardization leads to varying usage of practices, tools, and certifications among different agencies across states. Without a federal regulation, states essentially decide their own standards in digital forensics.

Each cause focuses on a method of control, whether it be a lack or increase. Although the inclusion of the USA-Patriot Act does not restrict an investigator's conduct, it still controls their authority; in this case, their authority is expanded. Regardless, with the causes combined together, they dictate the field of digital forensics more than digital forensics dictates itself. For digital forensics to revolutionize its certifications, procedures, and tools, legal guidelines must first allow it.

Ch. 13: "Reflecting On, Testing, and Communicating the Understanding or Theory"?

Although this research dives into law, criminology, and computer science, there are many ways to build upon this work. Firstly, a thorough examination and review is required for

computer science; the focus should be centered around specific changes or updates in devices and digital forensic tools. The main objective is to understand which types of changes are tolerable enough to pass guideline restrictions (e.g., Daubert Standard). Furthermore, one should review literature from the discipline of information technology to study how digital forensic investigators may handle networks and packets during investigations. Using the Newell Test, this research fulfills each question. The new understanding allows for more effective action, answers the research question, and potentially proves itself useful to policymakers and practitioners interested in digital forensics.

If one visualizes digital forensics as a double-edged sword, then legal guidelines are the tools that can sharpen or blunt it. Acts, such as the USA-Patriot Act, can cut deep into the privacy of both criminals and normal citizens. Alternatively, the right for an individual to have privacy can blunt the efficacy of criminal investigations. Although digital forensics is treated as an "art" compared to other forensic sciences, it is an "art" that determines people's lives. Digital forensic investigators must understand that rules and guidelines bind them because their practice can easily incriminate or absolve defendants. As for policymakers and legislators, they must understand that their policies dictate how digital forensics is conducted, which affects everyone, including themselves. Prejudice and self-interest have no place in a practice that upholds justice.

Conclusion

Legal guidelines and issues regarding privacy dictate digital forensics as a whole. Guidelines, such as the Federal Rules of Evidence, force investigators to follow procedures during investigations. Investigators must use industry-standard tools while collecting and analyzing evidence to ensure admissibility. Privacy restricts the scope of investigations and the

authority of investigators. The ability for state agencies to set their own standards can potentially discredit digital forensics as a valid scientific discipline, rendering collected evidence as inadmissible. Future policies can restrict or increase developments in digital forensic tools and how investigations are conducted.

References

Adams, C. W. (2008). Legal issues pertaining to the development of digital forensic tools. *2008 Third International Workshop on Systematic Approaches to Digital Forensic Engineering*, 123–132. https://doi.org/10.1109/SADFE.2008.17

Dehghantanha, A., & Franke, K. (2014). Privacy-respecting digital investigation. *2014 Twelfth Annual International Conference on Privacy, Security and Trust*, 129–138. https://doi.org/10.1109/PST.2014.6890932

Manes, G. W., & Downing, E. (2009). Overview of licensing and legal issues for digital forensic investigators. *IEEE Security & Privacy* (Vol. 7, Number 2, pp. 45–48). https://doi.org/10.1109/MSP.2009.46

Ryan, D. J., & Shpantzer, G. (2002). Legal aspects of digital forensics. http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf

Vincze, E. A. (2016). Challenges in digital forensics. *Police Practice and Research*, *17*(2), 183–194. https://doi.org/10.1080/15614263.2015.1128163

Zahadat, N. (2019). Digital forensics, a need for credentials and standards. *The Journal of Digital Forensics, Security and Law*, *14*(1). https://doi.org/10.15394/jdfsl.2019.1560