An Analysis of Legal and Constitutional Rights Affecting Computer Forensics and Collection of Evidence

Corinne Otten

Department of Computer Science, DePaul University

CSEC 477: Governance Policies in Information Assurance

Professor Andy Reeder

June 16, 2024

An Analysis of Legal and Constitutional Rights Affecting Computer Forensics and Collection of Evidence

Abstract

You're watching a movie. There's been a murder. The police have a suspect in mind who may or may not have been with the victim during the crime. The location data, messages, and call log could be crucial evidence necessary to convict this suspect. However, there is only circumstantial evidence indicating that the suspect was there; no direct witnesses were found. The suspect refuses to unlock their phone, citing privacy rights. It's a catch-22. The police cannot compel them to unlock their phone without violating constitutional protections against unreasonable searches, but the information on the phone can definitively determine whether the suspect was even there at the time. Whose side are you on?

Keywords: computer forensics, digital forensics, digital data, evidence collection, criminal investigation, legal frameworks, constitutional rights

Introduction

This paper examines the intersection of legal frameworks and constitutional rights with the current practices of using computer forensics to collect evidence that will later be used by law enforcement or the courts for criminal proceedings. The complexities of maintaining this balance are numerous. As individuals, it is perhaps natural to advocate for personal privacy and confidentiality of data, especially if that information will be used by the government. However, as a victim of a crime, it is perhaps natural to want to avoid impediments to the digital collection of evidence and use of computer forensics to catch the culprit. It is interesting that many people advocate for privacy and limiting access of their confidential data to government or law enforcement until they, themselves, are a victim of a crime. As a victim, they often expect the police to be able to access all of a suspect's digital information from their laptops, cell phones, car GPS, etc. with no impediment. How can the government and judicial system continue to advocate for the individual's legal and constitutional rights to privacy while also using all resources available – including digital data – to keep society safe and free from harm?

Thesis

This paper will highlight the complexities and challenges that use of computer forensics by law enforcement, in particular, raises for individual privacy rights. The use of computer forensics in collection of evidence is imperative to modern criminal investigations. Due to the advances in technology, huge amounts of information can be created, stored, and accessed digitally and there are many sources that illustrate the clear benefit to having so much information to obtain convictions (Goodison et al., 2015). However, in the United States, every

individual has certain legal and constitutional rights to privacy. Law enforcement must balance these two opposing forces for justice to be equitable.

Preview

In this paper, I will answer the following questions:

1. What is computer forensics and how is it used to collect evidence in a law enforcement investigation?
2. What are the legal frameworks and constitutional rights that govern computer forensics and digital evidence?
3. What are the ethical and practical challenges in using computer forensics?

Computer Forensics Definition and Background

According to the National Institute of Standards and Technology (NIST), computer forensics is "the application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony" (CSRC Content Editor, n.d.). Digital evidence is any digital data that is retrieved and analyzed so that it can be useful in criminal investigations. Typically, this includes digital information collected from such devices as computers, external hard drives, mobile phones, car GPS, video and surveillance cameras, or any other devices storing digital data. In terms of computer and digital forensics, the digital information is collected from these devices, stored, analyzed, and presented as evidence in legal proceedings.

The Existing Legal Framework Governing Computer Forensics

Constitutional Amendments

The Fourth and Fifth Amendments to the United States Constitution protect the individual against misuses of computer forensics, ensuring that digital searches and seizures are conducted lawfully and that individuals are not compelled to incriminate themselves through decryption. In general, the Fourth Amendment protects individuals against unreasonable search and seizure of evidence and promotes the concept of a reasonable expectation of privacy. This amendment requires law enforcement to obtain a warrant judicially sanctioned and supported by probable cause before accessing digital devices and data. The Fifth Amendment protects an individual against self-incrimination, stating that no person "shall be compelled in any criminal case to be a witness against himself." In reference to computer forensics, the act of decrypting data can be considered testimonial because it requires the individual to reveal the existence, possession, and authenticity of potentially incriminating evidence. Essentially, these amendments have been extended to the collection of and access to digital evidence during investigations in the same manner they apply to physical evidence.

Federal and State Laws

There are several key federal and state laws that have contributed to the regulation of electronic evidence gathering. Two such federal laws are the Electronic Communications Privacy Act (ECPA) and the Computer Fraud and Abuse Act (CFAA). The ECPA, enacted in 1986, protects wire, oral, and electronic communications while in transit and while stored, making it illegal to intercept or access such messages without proper authorization. This law ensures that electronic communications, such as emails and phone calls, are afforded the same privacy

protections as physical mail and in-person communications. The CFAA, also enacted in 1986, plays a vital role in protecting against unauthorized access to computers and electronic data by making it illegal to access a computer without proper authorization, access digital information that exceeds that which is specifically authorized, and obtain information from a protected computer. Together, these and similar laws regulate how law enforcement can obtain and access electronic and digital data during investigations.

Case Law

There are several legal cases that have set case law precedent regarding certain aspects of computer forensics. Riley v. California (2014), for instance, was a landmark Supreme Court case that set a precedent that digital data on cell phones cannot be searched without a warrant. In Carpenter v. United States (2018), the Supreme Court ruled that accessing historical cell phone records that provide a comprehensive history of the user's past movements requires a warrant, thus expanding the Fourth Amendment protections to include the privacy of location data. The In re Grand Jury Subpoena Duces Tecum (2012) case reinforced the idea that individuals cannot be compelled to provide decrypted digital data, by being forced to decrypt a device storing digital data, if it is deemed testimonial.

The Ethical and Practical Challenges of Using Computer Forensics

Ethical Challenges

There is a perpetual societal debate regarding the importance of the rights of an individual to digital privacy and the needs of law enforcement to access an individual's digital data to protect society. The legal frameworks discussed above are designed to mitigate potential abuses of these privacy rights by law enforcement. For instance, a search warrant

must be obtained before collection of evidence, including digital data. However, the search warrant only applies to the suspect and the property in question. Physical searches are often limited in scope by the physical boundaries of the property or items being searched. In contrast, digital devices store vast amounts of personal data far exceeding what might be found in a physical space. The case of Riley v. California highlighted that searching a cell phone is far more intrusive than searching a wallet or a purse due to the extensive amount of personal information stored within.

Similarly, the information gathered from a physical item or space would have far less overlap between the suspect and other third parties they have communicated with who are in no way connected to the investigation. For instance, the Doordash employee, Bob, who delivered their lunch yesterday. Bob's full name and personal information are in the Doordash app that was scraped of digital information, legally, in accordance with a search warrant issued for the suspect's mobile phone. Was a search warrant also obtained to gather Bob's personal information? Was Bob even notified? As expressed by Thompson and Warzel (2020) in the New York Times article "Twelve million phones, one dataset, zero privacy",

> For many Americans, the only real risk they face from having their information exposed would be embarrassment or inconvenience. But for others, like survivors of abuse, the risks could be substantial. And who can say what practices or relationships any given individual might want to keep private, to withhold from friends, family, employers or the government?

A suspect in a criminal investigation may have their historical location data protected by the Fourth Amendment, but what about the digital data of third parties who have had peripheral

contact with the suspect and are not themselves being investigated? Individuals visiting mosques, churches, abortion clinics, queer spaces, and other sensitive areas are just as deserving of location protection, and yet their location on any given day could be obtained by law enforcement in connection with an investigation through no wrongdoing or fault of their own.

Practical Challenges

The application of these protections to digital evidence creates unique challenges in maintaining data integrity, availability, and confidentiality due to the ever-evolving nature of digital data, its volume, and the means of accessing it. Just as physical evidence can be tampered with, so too can digital evidence. Yet, unlike digital evidence, access to physical evidence collected in an investigation is rather limited. If physical evidence is stored at the precinct in a secure physical evidence locker, the number of individuals who have access to that area should be rather small – or at least monitored. And, if the area was broken into by an unauthorized party, it would be difficult to widely distribute any physical items obtained. On the contrary, even with secure hardware and software protections, it only takes the unauthorized access of one individual to distribute digital data to the entire world online.

There does exist a general sense of an industry-standard for professional collection, storage, and accessing of digital data, but there is no federal or state official standard. This means that it is up to each precinct and/or corporation performing computer forensics to keep up to date with the various Constitutional, federal, state, and case laws to ensure that they are handling digital data in accordance with the laws and regulations that apply to them. This requires a vast amount of oversight and expertise that most precincts do not seem to possess (Belshaw, 2023). It seems that most precincts only have one or two people that may or may not

be fully devoted to the task of computer forensics, and even then it is unclear whether they have been adequately trained for the task.

Assuming industry-standard and professional security of digital evidence is being used, what guarantee does the court have that the digital evidence presented in court has not been modified – either by the owner or by those who collected and analyzed it? How can anyone be sure that the chain of custody is accurate and that the original image preserved was the original and had not been already modified? Where does law enforcement house the digital data gathered and who has access to it? If individuals who are legally allowed to access the digital evidence view confidential information, legally, what assurances are there that those individuals won't disclose that confidential information or use it to their own benefit? And, what happens to the digital data after the investigation is completed? What if a suspect is found innocent: should their confidential information and digital data be kept by the police on a server in their precinct? In such a case, is there an avenue for requesting that the digital data, in whole or in part, be deleted and removed from all police storage devices?

Conclusion

I do not know the answer to the above questions, but I do know that the proper balance between individual privacy and law enforcement efficacy when it comes to the use of computer forensics in the collection of digital data is a challenge that is ongoing, a legal issue that is hotly contested, and a goal whose goal post is continually moving. To keep up with the evolution of digital data and the means to collect and access it, we must adapt the laws and requirements regarding computer forensic use in digital data collection to ensure the fundamental privacy

rights of the individual are maintained. Specifically, as new technologies develop and evolve, so too must the definitions of related words in Constitutional Amendments evolve. For example, the definition of “search” in the Fourth Amendment has changed many times over the years and will need to continue to change as the fundamental concept of that word expands (Slobogin & Brayne, 2023). Ultimately, this balancing act will remain constant and something that requires the attention of every United States citizen.

References

Belshaw, S. (2023). *Next generation of evidence collecting: The need for digital forensics*. University of North Texas. Retrieved from https://files.eric.ed.gov/fulltext/EJ1341743.pdf

CSRC Content Editor. (n.d.). digital forensics - Glossary | CSRC. https://csrc.nist.gov/glossary/term/digital_forensics

CISA. (2018, June 21). Securing Network Infrastructure Devices | CISA. Www.cisa.gov. https://csrc.nist.gov/glossary/term/digital_forensics

Digital Evidence and Cloud Forensics: Contemporary Legal Challenges. (2023). *MDPI*. Retrieved from https://www.mdpi.com/2078-2489/12/5/181

Garfinkel, S. (2013). Digital forensics. *Wiley Interdisciplinary Reviews: Forensic Science*, 1(3), e1240. https://doi.org/10.1002/wfs2.1240

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015, April 20). *Digital evidence and the U.S. Criminal Justice System: Identifying technology and other needs to more effectively acquire and utilize digital evidence*. RAND. https://www.rand.org/pubs/research_reports/RR890.html

Legal issues in computer forensics and digital evidence. (n.d.). *Academia.edu*. Retrieved from https://www.researchgate.net/publication/344695331_Legal_Issues_in_Computer_Forensics_and_Digital_Evidence_Admissibility

Slobogin, C., & Brayne, S. (2023). Surveillance technologies and Constitutional law. *Annual Review of Criminology*, *6*(1), 219–240. https://doi.org/10.1146/annurev-criminol-030421-035102

Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law and Security Report/Computer Law & Security Report*, *49*, 105801. https://doi.org/10.1016/j.clsr.2023.105801

Thompson, S. A., & Warzel, C. (2020, January 26). Opinion | Twelve million phones, one dataset, zero privacy. *The New York Times*. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html