Global Information Assurance Certification Paper

Logon Banners

GIAC (GLEG) Gold Certification

Author: Mr. Keelan T. Stewart, keelan.t.stewart@gmail.com
Advisor: Chris Walker, CISSP, CISA, GSEC
Accepted: February 24, 2019

Abstract

Logon banners have been a common feature of operating systems and applications for many years. Organizations have adopted logon banners for a myriad of purposes, from threatening unauthorized users with severe repercussions to informing employees that they should not have an expectation of privacy on workstations. The impetus for logon banners typically comes from executive leadership or the legal department, often in response to an incident or lawsuit where such a disclaimer could have aided their stance. Drafting a comprehensive logon banner is daunting, especially when assigned to an arbitrary department with an expectation of quick completion. Understanding the common elements of a logon banner and having a framework to identify requirements, select elements, and write the text allows anybody tasked with implementing a logon banner to do so correctly the first time. This paper considers laws and legal topics from the perspective of the United States and may not be applicable to other jurisdictions.

DISCLAIMER: I am not an attorney. This paper is for information only and should not be taken as legal advice. If you require legal advice on this topic, consult your attorney.

1. Introduction

Litigation surrounds organizations impacted by cyberattacks, making them both the plaintiff and defendant. Breaches of third-party information result in audits and investigations to determine if the organization did enough to reasonably protect the information. Lawsuits against cyber criminals and negligent vendors seek to recover damages from responsible parties. Logon banners are used to address both situations, demonstrating the organization takes reasonable steps to protect information and establishing a legal boundary to outside parties.

Logon banners are the virtual equivalent of a "No Trespassing" sign. The case law surrounding logon banners is inconclusive; however, they are a common directive from general counsel to support their efforts with litigation. Logon banners, due to their low cost, are typically deployed in a belt-and-suspenders approach, meaning they are used as a redundant control to reinforce other security controls that protect information and establish legal boundaries. Logon banners should not be used as the sole control for these purposes, just as a "No Trespassing" sign does not alleviate a bank from having a locked vault to protect money.

The use of logon banners has spread from the public to the private sector. Government agencies, especially law enforcement and the military, were among the first organizations to implement logon banners. Often the target of dedicated cyberattacks, these agencies sought to establish their right to investigate and prosecute cyber criminals, while avoiding legal issues that could arise based on an expectation of privacy and due process of law. Government logon banners, seeking to assuage these concerns, often cite specific sections of the law that establish their legitimacy to monitor and prosecute unauthorized users. Private sector organizations, not bound by the constitutional rules imposed on government and law enforcement agencies, have adopted a myriad of logon banner approaches, ranging from simple notices to complex, contract-like agreements. The purpose and wording of logon banners depend on the laws and regulations to which the organization is subject.

Mr. Keelan T. Stewart, keelan.t.stewart@gmail.com

1.1. Computer Crime Laws

Understanding the history of computer crime laws aids in developing a logon banner that facilitates legal recourse against malicious actors. Computer crime laws broadly fall under three types of law: privacy, property, and trade. Privacy laws are the most commonly associated with computer crimes and have to do with the constitutional right to privacy granted by the Fourth Amendment. Property laws are used to seek restitution for damages caused by the misuse of systems or fraud perpetrated using stolen information. Trade laws may be used by and on behalf of the public against organizations that misrepresent their activities in ways that cause harm to their consumers, whether privacy or property related.

1.1.1. Fourth Amendment to the United States Constitution (1791)

The constitutional right to privacy, established in the Fourth Amendment, limits the ability of government agents to search a person's property where a reasonable expectation of privacy exists (U.S. Const. amend. IV). This restriction applies to agents acting on behalf of the government, whether federal, state, or local (*Mapp v. Ohio*, 1961). Fourth Amendment protections extend to telephone conversations (*Katz v. United States*, 1967), stored electronic data (*United States v. Heckenkamp*, 2007), and electronic communications (*United States v. Warshak*, 2010). The primary motivation for government logon banners is to reject any expectation of privacy, thereby establishing authority to monitor use and prosecute unauthorized users.

1.1.2. The Communications Act (1934)

State laws were responsible for the privacy of telegraph and telephone communications throughout the nineteenth century, banning the use of wiretapping by both private parties and the government (Kaplan, Matteo & Sillett, 2012). In legislation aimed at regulating the AT&T monopoly, the federal government made the divulging of information gained through wiretapping illegal (The Communications Act of 1934). The law did not make wiretapping illegal but focused on the divulging of information, including using it as evidence before a court. Excluding wiretap evidence was the first step in establishing an expectation of privacy beyond physical locations, which was the standard for prior cases of illegal search and seizure (*Olmstead v. United States*, 1928).

1.1.3. Federal Wiretap Act (1968)

Court rulings following The Communications Act of 1934 further restricted law enforcement's use of wiretapping by extending constitutional expectations of privacy to state courts (*Mapp v. Ohio*, 1961) and searches of intangible property (*Katz v. United States*, 1967). Public interest in crime control increased during the War on Drugs in the 1960s, leading to legislation that permitted wiretapping with a warrant (Title III of the Omnibus Crime Control and Safe Streets Act of 1968). The law, commonly referred to as the Federal Wiretap Act, also made it legal for any party of a conversation to record or consent to the recording of a conversation, with or without the knowledge or consent of any other party (Title III of the Omnibus Crime Control and Safe Streets Act of 1968).

1.1.4. The Computer Fraud and Abuse Act (1984)

At the height of the Cold War, movies such as *WarGames* (Goldberg et al., 1983) had a profound impact on the national discourse around computer crimes and national security. The Computer Fraud and Abuse Act, part of a larger set of legislation to reform crime control, made it illegal to gain unauthorized access to a computer (Comprehensive Crime Control Act of 1984). Related is the civil tort of trespass to chattels, which in the digital context is the unauthorized use of a computer in such a way that it causes damages to the owner, whether by disabling or degrading service or stealing something of value (American Law Institute, 1965). Establishing when access is unauthorized is the principal issue addressed by implementing a logon banner.

1.1.5. Electronic Communication Privacy Act (1986)

Expanded use of networked personal computers necessitated clarification of expectations of privacy. Amendments to previous laws included protections for electronic and stored communications, including personal communications in the workplace (Electronic Communications Privacy Act of 1986). Employers generally have free use to monitor their systems for performance, bona fide business purposes, and enforce company policy but they do not, per se, have free reign to monitor an employee's personal communications without just cause. Acceptable use policy should address issues related to employee monitoring, not logon banners, as there is generally more standing in a signed agreement than a click-through logon banner.

1.1.6. USA PATRIOT Act (2001)

Following the terrorist attacks on September 11th, 2001, and acknowledging the widespread adoption of the Internet, new legislation greatly expanded the government's authority to investigate threats to national security (USA PATRIOT ACT of 2001). The Patriot Act, as it is commonly known, updated laws regarding telephone and electronic communications with procedures for the collection of evidence without the knowledge or consent of the owner or subject (USA PATRIOT ACT of 2001). Information stewards need not notify nor obtain consent for monitoring of information in association with evidence requests made under the Patriot Act (USA PATRIOT ACT of 2001).

1.1.7. Fair Trade Laws

While privacy and property laws encompass the majority of codified law about computer crimes, often fair trade laws are how organizations are held accountable for their actions or negligence in cyberspace. Federal and state laws ban "unfair or deceptive acts or practices in or affecting commerce," (Federal Trade Commission Act of 1914). Not complying with self-imposed, publicly available policies and procedures, such as a privacy policy, are generally considered unfair and deceptive. Ashley Madison, the victim of a data breach in 2015, had stated that they protected users' personal information but was shown to have unreasonable security in place, resulting in the Federal Trade Commission bringing suit against them for unfair and deceptive trade practices ("Privacy & data security update (2016)", 2017).

1.1.8. State Privacy Laws

All states have a breach notification law that pertains to the privacy of personal information about citizens. Most states have laws that protect information collected about their citizens by any organization while other laws only apply to organizations that conduct business within the state. State laws use broad language similar to fair trade laws, often with requirements for maintaining reasonable security and written security policies. Some states, such as Connecticut (Conn. Gen. Stat. § 31-48d) and Delaware (Del. Code § 19-7-705), require written notice from employers before they can monitor employees. These notices are best adopted in a signed acceptable use policy, not through a logon banner.

1.2. Criminal Elements

Establishing that a crime has taken place requires the plaintiff to demonstrate that the three elements of a crime occurred: a criminal act, criminal intent, and the concurrence of those two events (Legal Information Institute, 2019). Understanding criminal elements and their relationship to computer crimes is important for understanding the intent behind and proper execution of a logon banner.

1.2.1. *Actus Reus* – Guilty Act

Prosecuting a crime involves proving that an individual physically carried out an illegal action. It is often fairly straightforward to prove that a criminal act occurred concerning computer crimes, as long as adequate and properly secured logs exist. The difficulty typically is identifying the individual who perpetrated the action and having the ability to find and prosecute the individual based on legal jurisdictions. It is not necessary to state the computer crime laws an individual may break when performing unauthorized actions on a system as ignorance of the law is not a defense.

1.2.2. *Mens Rea* – Guilty Mind

Proving an individual's criminal intent is often the more difficult part of prosecuting a crime. On the one hand, computer crimes involve a demonstration of technical skill that is often sufficient to establish criminal intent if the *actus reus* exists. On the other hand, as more attacks are scripted and sold inexpensively on the Internet, would-be hackers may launch attacks and be unaware of their true scope or scale.

Logon banners are a traditional method for establishing *mens rea* by requiring the user to explicitly take action to acknowledge that they are accessing a system owned by an organization. While the existence of a logon mechanism has been found to be a factor in establishing an expectation of privacy and therefore preclude unauthorized access (*United States v. Lucas*, 2011), a logon banner provides a belt-and-suspenders approach to demonstrate that a person accessing a system without authorization was aware of and intentionally acted to gain unauthorized access.

2. Logon Banner Implementation

The process for designing a logon banner involves understanding the elements of a logon banner, what regulations require logon banners, and how to draft the logon banner. Technical implementation of a logon banner is platform-specific and outside of the scope of this document; however, it is typically a straightforward process.

2.1. Logon Banner Elements

Logon banners take many forms, from a single sentence to multi-page legal documents that require you to scroll through its entirety before you can advance. Though the language can vary among organizations and industries, common elements emerge. The following is an overview of these common elements and a synopsis of whether or not to include them in a logon banner.

2.1.1. Ownership

Statements of ownership establish a legal boundary for a computer. This statement should read: "this computer is the property of [company]." It is preferable to use the word "computer" instead of "system" or a more technical term, as "computer" is the word used in most legislation and court findings. As for the name of the company, it is the preference of the organization's legal counsel whether to use the formal business name or the "doing business as" name as both are acceptable. The statement of ownership should always be included in a logon banner as it is difficult to establish what authorized access means without knowing who has legal authority to authorize access.

Secondary statements of ownership are required for shared organizational resources or cloud service architectures. Consider an organization which owns its computers and data but not the network or federated services, which is a standard architecture for subsidiaries. In this case, the statements of ownership should be: "this computer is the property of Subsidiary Co. This network is the property of Holding Corp." Similar statements would be appropriate for cloud architectures, using plain language instead of technical jargon: "this service is the property of Sample Co. This computer is the property of Cloud Service Co."

2.1.2. Prohibition

Statements of prohibition establish what actions are authorized or not. This statement should read: "unauthorized access is prohibited." The acceptable use policy should define authorized access and be signed as acknowledged by anybody with authorized access to the system. The acceptable use policy helps solve legal issues around authorized users who perform unauthorized actions. Limiting the terms in the logon banner also helps avoid unauthorized users from finding a legal loophole to justify or explain their actions as legal. The statement of prohibition should always be included in the logon banner to reserve rights for accessing the system.

2.1.3. Scope

Statements of scope identify the boundary of the system to which the logon banner applies, typically reading: "…including all equipment, networks, devices, logs, etc." Determining the scope of a system can be difficult. Explicitly stating the scope implies that anything not listed is outside of the scope and therefore fair game. Avoid including scope statements in a logon banner. The better approach is to have logon banners on any access point to systems, where there should already be logon mechanisms, to demonstrate that all access requires authorization. As with the statement of prohibition, not specifying a scope reserves the right to argue the scope if necessary.

2.1.4. Audience

Many logon banners attempt to define the specific audience to which the banner applies, with language such as: "…user, including employees, contractors, vendors, customers, etc." The purpose of this audience scope comes from a desire to reinforce that the logon banner applies not only to the organization's employees but also third-party affiliates. The problem is, as with the technical scope, having an explicit list implies that omitted parties are not subject to the terms of the banner. The acceptable use policy is the best place to address issues that affect different classes of users, such as employees and vendors, rather than attempting to address all of them in the logon banner.

A note on audiences: while drafting the logon banner, remember that the ultimate audience of a logon banner is a judge or a jury, which is why plain language is preferred.

2.1.5. Monitoring

Monitoring consent statements advise the user that further access may be monitored and establish that the user should not expect privacy. A monitoring statement might read: "…may be monitored, recorded, or subject to audit." Some organizations, typically government and law enforcement, are required to have monitoring consent statements by their regulators. For other organizations, it is not necessary to state that monitoring may occur if it is legal without consent, such as monitoring a website to ensure proper functionality.

Exception cases arise with regards to employee expectations of privacy. Ownership plays a principal role in determining expectations of privacy (*United States v. Lyons*, 1993). While this generally gives employers a degree of authority to monitor their systems and employees, circumstances can arise where an employee's expectation of privacy is legitimate, such as accessing a private email system on an employer's computer (*Stengart v. Loving Care Agency, Inc.*, 2010). It is best to disclaim expectations of privacy in the acceptable use policy, which can more accurately represent situations where exceptions are required by law.

2.1.6. Enforcement

The enforcement clause of a logon banner describes what actions the system owner may take if unauthorized access occurs. Enforcement clauses may read: "…subject to disciplinary action, civil or criminal charges." It is not necessary to state that crimes may be subject to civil or criminal charges. The acceptable use policy should address disciplinary actions, not the logon banner.

2.1.7. Evidence

Evidence gathering consent statements seek to establish authority to gather evidence of user actions, stating: "evidence may be provided to law enforcement." As with the enforcement clause, it is not necessary to state that an organization may respond to lawful requests for evidence. Furthermore, the legal burden in such a dispute would be on the law enforcement agency requesting the evidence, not the organization. If legal counsel believes this statement is necessary, include it in the acceptable use policy.

2.1.8. Consent

Statements of consent indicate that the user has read the logon banner and consents to the terms, taking on more of a contractual tone like: "by continuing, you consent to these terms." There is no consensus on the legal standing of banners and pop-up boxes for contractual agreements, given that authentication occurs afterwards. Issues that involve a bona fide consent requirement, such as monitoring, should be conveyed in the acceptable use policy and signed by the user, not in a logon banner or notice.

2.1.9. Deterrence

Statements of deterrence encompass all explicit or implied threats to convince a user not to gain unauthorized access. Deterrence statements may cite specific laws, prison terms, and fines, similar to those found on FBI anti-piracy warnings at the beginning of films. Deterrence as a concept is often difficult to measure and of questionable effectiveness. The international nature of computer crimes also makes these threats difficult, as they may not be enforceable in other jurisdictions. Unless required by regulation, avoid statements of deterrence for brevity.

2.2. Regulations

Most laws are intentionally vague to permit flexibility of implementation over time. Regulatory and judicial bodies interpret the law, occasionally providing specific guidance in the form of standards, directives, findings, and opinions. Regulators are typically industry-specific and include both government and private organizations. Private regulators, such as the Payment Card Industry Security Standards Council, may be used for competitive advantage (a seal of approval) or to satisfy contractual obligations (contracts with credit card processors).

The National Institute of Standards and Technology (NIST), an agency under the Department of Commerce, is responsible for creating technical standards for all government agencies to follow. NIST Special Publications (SPs) are comprehensive and solution-agnostic, leading to their adoption by many private organizations as industry best practices. Several NIST SPs provide industry-specific security controls to satisfy legal and regulatory requirements.

2.2.1. Federal Agencies

All federal agencies, state agencies that share information, and contractors that provide services on behalf of the government are required to implement an information security program (Federal Information Security Modernization Act of 2014). The law gives authority for defining security requirements to NIST, who published a set of security controls and implementation guide (NIST SP 800-53 R4, 2013). FISMA requires organizations to have a system use notification with the following elements: ownership, prohibition, monitoring, and consent (NIST SP 800-53 R4, 2013).

FISMA requires a baseline set of security controls and many federal agencies have supplemental controls or offer specific guidance for implementation. The requirements vary by the sensitivity of the information the agency handles; in general government banners tend to be lengthy and cite applicable laws. The Nuclear Regulatory Commission mandates the following:

I UNDERSTAND AND CONSENT TO THE FOLLOWING:

I am accessing a U.S. Government information system provided by the U.S. Nuclear Regulatory Commission (NRC) for U.S. Government-authorized use only, except as allowed by NRC policy. Unauthorized use of the information system is prohibited and subject to criminal, civil, security, or administrative proceedings and/or penalties.

USE OF THIS INFORMATION SYSTEM INDICATES CONSENT TO MONITORING AND RECORDING, INCLUDING PORTABLE ELECTRONIC DEVICES.

The Government routinely monitors communications occurring on this information system. I have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search, or seize any communication or data transiting or stored on this information system.

Any communications or data transiting or stored on this information system may be disclosed or used in accordance with federal law or regulation.

REPORT ANY UNAUTHORIZED USE TO THE COMPUTER SECURITY INCIDENT RESPONSE TEAM (301-415-6666) AND THE INSPECTOR GENERAL.

Figure 1: NRC Logon Banner (Nuclear Regulatory Commission, 2017).

Government agencies have the prerogative to operate in formal, transparent manner to satisfy civilian oversight. Lengthy logon banners have the disadvantage of being ignored by the user, creating less legal standing than a succinct message. When not required to do more, it is best to keep logon banners as brief and direct as possible.

2.2.2. Law Enforcement

Given the constitutional right to privacy, law enforcement agencies have special requirements for ensuring that people are aware of their rights. The Federal Bureau of Investigation, through information sharing agreements, regulates state and local law enforcement agencies that handle federal criminal records (Criminal Justice Information Systems, 2010). The requirements elements are the same as FISMA: ownership, prohibition, monitoring, and consent (Federal Bureau of Investigation, 2017).

2.2.3. Financial and Retail

Private, for-profit organizations often eschew regulatory oversight, as it adds overhead and diminishes the bottom line. The major financial laws require privacy policies but not a logon banner (Sarbanes-Oxley Act of 2002; Gramm-Leach-Bliley Act of 1999). Retails who accept major credit cards are contractually obligated to comply with the Payment Card Industry (PCI) Data Security Standard, which specifies security controls based on the type and volume of transactions conducted but also does not require a logon banner (PCI Security Standards Council, 2018).

2.2.4. Healthcare

Personally-identifiable health information has more legal protection based on its sensitive nature. Federal and state laws require a broad spectrum of security controls related to protected health information; however, none of them specifically require a logon banner (Health Insurance Portability and Accountability Act of 1996; Health Information Technology for Economic and Clinical Health Act of 2009; Unauthorized Access to Patient Medical Information, 2008). Many hospitals also participate in third-party assessments to validate HIPAA compliance, such as HITRUST or The Joint Commission. HITRUST requires that larger organizations (Level 2) have banners that have ownership, prohibition, monitoring, and consent elements (HITRUST, 2014). HITRUST requires government contractors to have banners that include ownership, prohibition, scope, monitoring, enforcement, evidence, consent, and deterrence elements (HITRUST, 2014). The Joint Commission does not require a logon banner (The Joint Commission, 2016).

2.3. Drafting a Logon Banner

The purpose of a logon banner is to support legal actions on behalf of the organization by providing reasonable assurance that a person gaining unauthorized access to a system did so knowingly and intentionally. To that end, logon banners should be written in unambiguous language and be concise to avoid users not reading it. Drafting a logon banner requires identifying requirements, selecting elements to satisfy those requirements, and reviewing and socializing the banner before implementation.

2.3.1. Identify Requirements

Logon banners have two principal requirement sources: regulations and the organization's general counsel. Legal and contractual obligations may specify language for logon banners; deconflict and integrate this language as much as possible. The general counsel may have specific concerns, typically based on previous lawsuits or incidents, which drive their requirements. Other stakeholders, such as IT, information security, and human resources, may further seek to expand or limit the scope of logon banners. When appropriate, ancillary stakeholders should be consulted and included to assuage their concerns. There may be more appropriate methods for addressing specific concerns, such as explaining any expectations of privacy in the acceptable use policy.

2.3.2. Select Elements

After identifying the requirements, select the elements that best address the requirements: ownership, prohibition, scope, audience, monitoring, enforcement, evidence, consent, and deterrence. The objective is to select the fewest number of elements possible while still addressing all of the requirements for the logon banner, avoiding scope creep and complexity. All logon banners should establish ownership and prohibit unauthorized access to establish a legal boundary. The remainder of the elements should be avoided when possible and used sparingly when necessary. The remaining elements may limit legal recourse, by creating loopholes, or may entice malicious action by challenging an unauthorized user. The default logon banner for most situations should be: "This computer is the property of [company]. Unauthorized access is prohibited," (Wright & Milone, 2017).

2.3.3. Review and Socialize

Stakeholders involved in the requirements identification phase should all be permitted to review the logon banner and provide feedback. Review presents another opportunity to address stakeholder needs, whether with the logon banner or alternate means. Scrutinize deviations from standard language for necessity and carefully consider diction from a legal and user perspective. After agreement on the final draft, socialize the logon banner with the entire user base before implementation. Socialization serves two purposes: 1) to identify any overlooked, unique situations that might require an exception; and 2) to inform the user base of a change that will be highly visible and persistent in their daily work life.

3. Conclusion

Logon banners are an effective, inexpensive security control that enhances the legal department's ability to litigate computer crimes. When unauthorized access occurs, logon banners establish a legal boundary and criminal intent. Logon banners provide a belt-and-suspenders approach to safeguarding information and seeking relief when deployed with other security controls to prevent and detect unauthorized use. Computer crime laws used to prosecute these actions stem from the constitutional right to privacy, property protection laws, and fair trade laws.

Several common elements exist within logon banners: statements of ownership, prohibition against unauthorized access, technical scope definitions, intended audiences, notices of monitoring activities, available enforcement actions, notices of evidence collection, agreements of consent, and threatening statements of deterrence. Legal regulations and contractual obligations may have specific language requirements; use anything beyond ownership and prohibition elements sparingly. The general framework for drafting a logon banner is to identify the requirements, select the appropriate elements, review the draft with all stakeholders, and socialize the logon banner before implementation. Less is more with logon banners. All organizations, public and private, should use logon banners to facilitate legal recourse and educate users, authorized or not, that the organization takes security seriously.

Mr. Keelan T. Stewart, keelan.t.stewart@gmail.com

3.1.1. References

American Law Institute. (1965). *Restatement of the law, second, torts 2d*. St. Paul, MN.

Comprehensive Crime Control Act of 1984, Pub. L. 98-473, 98 Stat. 1976, codified as 18 U.S.C. § 1 et seq.

Conn. Gen. Stat. § 31-48d.

Criminal Justice Information Systems, 28 C.F.R. Part 20 (2010).

Del. Code § 19-7-705.

Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848, codified as amended as 18 U.S.C. § 2510 et seq.

Federal Bureau of Investigation. (2017). *Criminal Justice Information Services (CJIS) security policy*. (CJISD-ITS-DOC-08140-5.6).

Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073, codified as 44 U.S.C. § 3501 et seq.

Federal Trade Commission Act of 1914, Pub. L. 63-203, 38 Stat. 717, codified as amended as 15 U.S.C. § 41 et seq.

Goldberg, L., Hashimoto, R., Schneider, H. K., & McNall, B. (Producers), & Badham, J. (Director). (1983). *WarGames* [Motion picture]. United States: United Artists.

Gramm-Leach-Bliley Act of 1999, Pub. L. 106-102, 113 Stat. 1338, 12 U.S.C. § 1831 et seq.

Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. 111-5, 123 Stat. 226, codified as 42 U.S.C. 201 et seq.

Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936, codified as amended as 45 C.F.R. Part 164.

HITRUST. (2014). *HITRUST common security framework* (Version 6.0).

Kaplan, H. J., Matteo, J. A., & Sillett, R. (2012). The history and law of wiretapping, 2012 Section of Litigation Annual Conference, Washington, D.C., 2012. Chicago: American Bar Association.

Katz v. United States, 389 U.S. 347 (1967).

Legal Information Institute. (2019). Criminal law. In *Wex*. Retrieved January 21, 2019, from https://www.law.cornell.edu/wex/criminal_law.

Mapp v. Ohio, 367 U.S. 643 (1961).

National Institute of Standards and Technology. (2013). *Security and privacy controls for federal information systems and organizations*. (NIST SP 800-53 R4).

Nuclear Regulatory Commission (NRC). (2017). *Warning banner standard*. (OCIO-CS-STD-0040).

Olmstead v. United States, 277 U.S. 438 (1928).

Payment Card Industry Security Standards Council. (2018). *Requirements and security assessment procedures* (Version 3.2.1).

Privacy & data security update (2016). (2017). Retrieved from Federal Trade Commission website: https://www.ftc.gov/reports/privacy-data-security-update-2016.

Sarbanes-Oxley Act of 2002, Pub. L. 107-204, 116 Stat. 745, codified as 15 U.S.C. § 7201 et seq.

Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (2010).

The Communications Act of 1934, Pub. L. 73-416, 48 Stat. 1064, codified as 47 U.S.C. § 151 et seq.

The Joint Commission. (2016). *Focused standards assessment tool*.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 197, codified as amended as 18 U.S.C. § 2510 et seq.

Unauthorized Access to Patient Medical Information, Cal. Health & Safety Code § 1280.15 et seq. (2008).

United States v. Heckenkamp, 482 F.3d 1142 (9th Cir. 2007).

United States v. Lucas, 640 F.3d 168 (6th Cir. 2011).

United States v. Lyons, 992 F.2d 1029, 1031 (10th Cir. 1993).

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. 107-56, 115 Stat. 272, 107th Cong., 1st Sess. (Oct. 26, 2001).

U.S. Const. amend. IV.

Wright, B., & Milone, M. G. (2017). Law of data security and investigations. In *Fundamentals of IT security law and policy* (p. 153). Bethesda, MD: SANS Institute

Mr. Keelan T. Stewart, keelan.t.stewart@gmail.com