De Jure Nexus Law Journal

Volume 3 | Issue 1 Art. 3

2023

ETHICS IN CYBER FORENSICS AND CYBER SECURITY IN UNITED STATES LEGISLATIONS

Ishaan Deepak Joshi

Recommended Citation

Ishaan Deepak Joshi, 'Ethics in Cyber Forensics and Cyber Security in United States Legislations' (2023) 3 DJNLJ 37-51.
Available at www.dejurenexus.com/vol-3-issue-1/.

ETHICS IN CYBER FORENSICS AND CYBER SECURITY IN UNITED STATES LEGISLATIONS

Ishaan Deepak Joshi[1]

ABSTRACT

The incidence of computer crime, defined as unauthorised access to a computer system, is increasing in recent times. Computer crimes encompass a variety of illicit activities, including hacking, phishing, cyber stalking, computer infections, and identity theft. As a result of technological progress, data at different institutions is now stored in computers rather than paper files. Individuals have discovered a method of accessing this information without authorization, with the intention of using it for their own benefit. In order to combat these negative aspects, the US legislature implemented legislation that incorporates ethical principles to safeguard critical data and maintain the protection of personal information. These laws encompass the Health Insurance Portability and Accountability Act, the Sarbanes-Oxley Act of 2002, and the Children's Online Privacy Protection Act of 1998. The mentioned acts include the California Database Security Breach Act of 2003, Computer Security Act, Privacy Act of 1974, Uniform Electronic Transactions Act, Electronic Signatures in Global and National Commerce Act, and Uniform Computer Information Transactions Act. All of these measures were implemented with the objective of safeguarding information in different departments from unauthorised access. Computer crimes can have detrimental consequences, including the manipulation, modification, and loss of critical information due to a computer system failure. Hence, it is imperative to implement safeguards that safeguard against these types of influences and protect the confidentiality of personal data.

[1] NALSAR University of Law and MIT-WPU Faculty of Law.

KEYWORDS

Data Privacy, Computer Forensics, Cyber Security, Ethics, US Legislations, Information Technology.

I. INTRODUCTION

The current incidence of computer crime is concerning, particularly with the emergence of the internet. Computer crime is the commission of a criminal act by the use of information technology to gain unauthorised access to a computer system, with the explicit purpose of unlawfully damaging, deleting, or altering data. Engaging in electronic plagiarism, data theft, and copyright manipulations are all acts that are regarded to be criminal offences.

In addition to causing physical damage, the unauthorised modification of private data and vital information, as well as the theft of software that involves tampering with privacy settings, is also regarded as a criminal act. In response to these criminal activities, security measures have been implemented to guarantee safety. These crimes can be classified into various categories, one of which is hacking. Hacking refers to the unauthorised intrusion into a digital system with the intention of illegally accessing stored information. The most prevalent offence is unauthorised access, which entails the divulgence of passwords and IP addresses in order to conduct business operations with an ambiguous identity.

Phishing refers to the act of acquiring sensitive information, such as usernames, passwords, and credit card numbers, by tricking users into providing them on well-known websites. Due to the trust placed in these websites, individuals are often enticed to provide valuable information. Cyber stalking involves the collection of user information from social networking sites like Facebook, chat rooms, and webpages, which is then used to harass the individuals. These actions might be categorised as

false allegations, threats, destruction of records & equipment, abusive phone calls, and obscene emails.

Computer viruses are malicious programmes that can erase files, propagate themselves, or cause a full system meltdown. They are transported via portable storage devices such as CDs, flash drives, and other similar media. Computer systems experience a complete failure and significant data loss as a consequence of virus infections. Identity theft refers to the fraudulent practise of assuming someone else's identity in order to illicitly access and withdraw funds from their accounts. This refers to the act of utilising another individual's credit card information or assuming someone's identity to acquire possessions that do not properly belong to the perpetrator. The aforementioned constitutes a compilation of discernible criminal activities in the present day. Information technology holds significant value, yet when utilised in certain ways, it can be regarded as a detriment.

II. THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

The US Congress passed this legislation in 1996 in response to the growing demand from patients to ensure the confidentiality of their health records. Title I of HIPAA focuses on providing health insurance coverage for workers in the event of job loss or a change in employment status. On the other hand, Title II, often known as Administration Simplification, is responsible for ensuring the security and anonymity of health records. Here, it is necessary to establish nationalised norms for the electronic healthcare industry, as well as identities for providers, health insurance policies, and employers. These procedures are designed to enhance the delivery of health care services.

Their improvement is achieved by the extensive implementation of electronic data sharing throughout the United States. Title II of the

Health Insurance Portability and Accountability Act delineates a range of transgressions related to healthcare and establishes the corresponding civil and criminal penalties for these violations. Additionally, it ensures protection against fraudulent activities within the health care system by mandating the Department of Health and Human Services to establish guidelines for the management and dissemination of health care-related data. Below are some of the regulations that exclusively pertain to the covered organisations.

Privacy guidelines primarily aim to regulate the utilisation and disclosure of information, particularly in the context of business transactions involving medical care providers and health insurers. Additionally, it examines the security measures around Protected Health Information. Disclosure of this information is only permitted to an individual after a 30-day period following their request, as mandated by law. An example of such a requirement would be in cases involving child abuse, where the information is necessary for welfare organisations. The transaction and code set rules pertain to healthcare providers who submit electronic filings. HIPAA facilitates the monitoring of their financial transactions.

Multiple Electronic Data Interchange formats are utilised in this transaction, including the EDI Health Care Claim Transaction set, EDI Retail Pharmacy Claim Transaction, and several more. The security rule pertains to Electronic Protected Health Information.[2] This document includes measures for administrative, physical, and technology security. An instance of a breach of HIPAA occurred when a health official in California, specifically in Los Angeles, accessed confidential documents of a celebrity and subsequently shared this information with tabloid publications. In this instance, individuals who were impacted were obligated to initiate legal proceedings with the Department of Health and Human Services. A severe penalty of at least 2.5k USD is imposed on

[2] Privacy rights clearing house.(2003). Web.

individuals who break this law, as it has the potential to endanger the health data of everyone.

III. THE SARBANES-OXLEY ACT OF 2002

This legislation focuses on the detection and regulation of fraudulent activities in financial statements. Instances of fraud have significantly impacted the global economy in recent times. This phenomenon is particularly noticeable in well-known and large corporations like the Enron Corporation and the WorldCom. The US legislature enacted legislation to safeguard investors from fraudulent activities by enhancing the accuracy and reliability of company disclosures.

The aforementioned corporations failed as a result of compensation strategies implemented by senior management and executives. These strategies aimed to generate significant profits by utilising liability receivers, such as special purpose entities, which effectively eliminated substantial amounts of debt from the balance sheet. Subsequently, they deserted the companies, resulting in the stockholders being left with no assets, hence contributing to the enterprises' downfall. Such actions diminish the confidence of shareholders in the stock markets.

Following the Enron disaster, the former US president George W Bush appointed senator Sarbanes and Congressman Mike Oxley to develop stringent regulations aimed at mitigating the likelihood of similar crises.

These laws are clearly stated in different sections of the constitution, including section 406 which mandates managerial executives to sign a code of code of conduct, section 409 which requires timely disclosure of changes in financial materials, and sections 802 and 1101 which prohibit

any alteration, destruction, or falsification of documented information to impede investigation on any matter.[3]

These measures, along with others, ensure that all corporations or shareholders in the US securities market adhere to the regulations set forth by the Sarbanes-Oxley Act.

IV. THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT, 1998

The legislation took effect in the United States on April 21, 2000. This pertains to the online collection of personal data by an operator from minors aged thirteen and below. The document clearly outlines the factors that an operator must consider when formulating a privacy policy, including the specific timing and method for obtaining information with the explicit consent of a parent or guardian. This legislation pertains to electronic services that are operated with the goal of generating profit. Children under the age of thirteen are required to provide information in this context. The Federal Trade Commission is responsible for establishing regulations and enforcing the Children's Online Privacy Protection Act. Additionally, it provides a safe haven for organisations such as TRUSTe, ESRB, CARU, and Privo. It establishes a graduated system that relies on parental agreement, ensuring responsibility for the manner in which information is obtained and the purposes for which it is utilised.

Those who violate COPPA regulations may face financial penalties. For instance, Xanga websites were required to pay a fine of a million USD for allowing children under the age of 13 to sign up for their service's multiple times without parental consent. Similarly, UMG Recordings was fined 400k USD for promoting Lil Romeo and endorsing children's games.

[3] Holt, F., M. (2008). The Sarbanes-Oxley Act: costs, benefits and business impact. Burlington: Butterworth- Heinemann.

Website operators should verify the identity of parents by utilising methods such as collecting credit card information, obtaining digital signatures by email, receiving completed consent forms by mail, or contacting them through a designated phone line. Adhering to these criteria ensures protection against the revelation of personal information by an individual concealing their status as a parent.[4]

V. THE CALIFORNIA DATABASE SECURITY BREACH ACT OF 2003

The purpose of this is to safeguard the personal information of citizens from being stolen and exploited by someone else to conduct a transaction while concealing their true identity. The legislation was implemented on 1 July 2003 and was well-received by the public in response to the rising incidents of identity theft at that time.

\The legislation pertains to entities responsible for safeguarding critical information, mandating them to promptly disclose any instances of criminal activity. This applies not only to firms located in California, but also to those outside of the state that are linked with it. The act also serves the purpose of notifying individuals about a suspected security breach, which is sometimes concerning since it can potentially harm a company's reputation and incentivize hackers who derive pleasure from inducing customer alarm.

This law also governs the control of sensitive information that is handled through the internet. Several measures have been implemented to ensure security, such as the installation of specific software that detects abnormal activity and blocks any unauthorised access to the server and gateways that monitor and prevent unauthorised access to personal

[4] Bro, H., R. (2004). The E-business legal arsenal: practitioner agreements and checklists. Washington, DC: American Bar Association.

information.[5] This statute also sponsors customer warnings regarding breaches through email and web posts. An exemplar of a security firm that provides such protection is the Andy Lawson and Southland shredding company.

VI. THE COMPUTER SECURITY ACT

The primary objective of the Computer Security Act of 1987 is to ensure the security and privacy of personal information within government computer systems. Additionally, the act provides guidelines and protocols to implement effective security measures. The enactment occurred through the Federal Information Management Act of 2002, specifically under section 305 (a), by the United States Congress. The statute defines sensitive information as data that, if lost, modified, or deleted without authorization, can have detrimental consequences on the reputation of the centralised system, perhaps resulting in a loss of public interest.

Historically, the legislation has failed to adequately ensure the security of this type of data in government networks, resulting in persistent challenges over its vulnerability. The provisions of this act include the establishment of the National Institute of Standards and Technology (NIST), which is responsible for creating and enforcing authorised regulations to protect information. Security protocols are implemented and the system's owners or users are obligated to receive training on the proper implementation of these measures. Regular and autonomous evaluation of the security plans is conducted to ascertain their effectiveness and compliance with the requirements of the Federal Information Security Act.

[5] Tendick, R. (2010). California Data Security Breach Act Helps Protect Private Information. Web.

FISMA mandates the creation of an incident center with the purpose of providing technical assistance to federal agencies in the identification, examination, and consolidation of federal data. Instances of federal computer crime encompass unauthorised access to a federal computer system, illicitly obtaining security, financial, or credit information from a state computer system, or transferring a code capable of causing harm to a safeguarded computer. All identified criminal activities are to be reported to the congress by means of a court-issued directive.[6] The federal government is not responsible for safeguarding information held in non-governmental systems. Consequently, the act does not classify unauthorised access to such material as a criminal offence, although it does mandate the protection of particular information inside the same non-governmental system.

An instance occurred in November 1999 involving the Social Security Administration, which manages a significant portion of the federal government's budget and was at risk of being hacked. In July, the Department of Transportation system was unlawfully breached via the internet, jeopardising sensitive information related to health, benefits, and other domains.[7]

VII. THE PRIVACY ACT ENACTED IN 1974

This measure was implemented in response to security concerns related to the creation and utilisation of computerised data. Four functional and substantive liberties were established in order to provide security. Firstly, a person can access information that is stored about them. Furthermore, it necessitated that the agencies adhere to prescribed laws in order to ensure fairness in their transactions. Furthermore, there are limitations on how agencies can disclose personal information to third parties. Finally, individuals have the ability to initiate legal proceedings

[6] Willemssen, J., C. (2000). Computer Security. Web.
[7] Oak, M. (2011). Types of computer crimes. Web.

against the state when their personal information is violated. The act also provides exemptions for certain instances in which personal information may be disclosed. These include situations where there is a necessity to enforce a law, where the information needs to be preserved in government archives for historical purposes, where statistical analysis is conducted by the census bureau, for routine administrative purposes within government agencies, and for investigative purposes.

With the progress of technology, personal information may now be stored in databases. However, this also increases the possibility of unauthorised access to this data. Therefore, it is necessary to have a law in place to assure security. In 1973, the Department of Health, Education and Welfare issued a report that mandated Congress to implement a code to guarantee equitable handling of personal information.

Personal details should not be kept confidential without a proper system in place. Individuals have the right to be informed about the information stored about them and the purposes for which it is intended. Individuals have the right to ensure that data collected about them is used solely for its initial objective and not for other reasons. Individuals have the right to rectify or modify the information stored about them. Any organisation responsible for maintaining discernible information should ensure its appropriate and lawful use.

The privacy act exclusively safeguards data within centralised systems. Noncompliance with this legislation incurs both civil and criminal consequences. These include the ability to file a lawsuit against an agency for denying access or refusing to update requested data. In such cases, the court may issue an order for amendment and require the US government to pay fees such as litigation and attorney's fees.[8] An individual or agency that deliberately solicits identifiable information

[8] The Privacy Act of 1974. (2009). Web.

about someone while concealing their true identity, retains this information confidentially, or divulges it without the owner's consent may be subject to a maximum fine of five thousand dollars.

VIII. UNIFORM ELECTRONIC TRANSACTIONS ACTS

The Uniform internet Transactions Act (UETA) was enacted in 1999 with the primary objective of mitigating obstacles to internet trade. In order to streamline ecommerce, a standardised signature was developed to address the issue of many states adopting different types of signing. The objective was to ensure the electronic signatures had an equivalent influence on the data as traditional paper signatures. Electronic signatures are linked to the electronic record, and anyone conducting transactions should utilise them. In this context, the term record refers to data that is kept digitally and may be accessed.

The act does not establish novel regulations, but rather promotes the incorporation of contracts, signatures, and records into electronic data. In the year 2000, with the implementation of the Electronic Signatures in Global and National Commerce Act, the United States Congress approved the Electronic Signatures in Global and National Commerce Act. The legislation pertains to individuals or entities who mutually consent to conduct their transactions by electronic means. This holds great significance as, when engaging in a business transaction, a signature is crucial for the purpose of clarifying and facilitating the tracking of payments. Merely receiving an email is insufficient as evidence of the agreed-upon terms and conditions.

The absence of a signature makes it more convenient for the party engaged to repudiate the agreed-upon terms of the transaction. Therefore, this evidence is crucial for ensuring seamless and equitable transactions. The legislation encompasses transactions pertaining to business, commerce, and the state. Section seven of this act permits the

utilisation of electronic signatures, documents, and contracts in commercial dealings, provided that there is a mutual agreement between the interested parties to employ them.

The legislation also aims to verify that the sender of an electronic item is the individual whose signature is utilised. This is referred to as attribution, as the signature is consistently attributed to the sender of the records. In accordance with UETA, timing is a factor that falls within its scope. A record is considered to have been delivered after it has reached the recipient in a format that can be comprehended by their computer system, or when the record is no longer in the possession of the sender.[9] UETA additionally guarantees that records are sent to the recipient's business premises or residence in the absence of a designated business premises.

IX. E-TECH AND ITS INFLUENCE ON THE NATION AND COMMERCE

The US legislature passed this legislation on 30 June 2000 with the purpose of facilitating the adoption of electronic records in both domestic and global corporate activities. The legislation guarantees the legitimacy of all internet business transactions. The law mandates that customer consent must be obtained in written form. This legislation was implemented in October 2000. The legislation permits the transmission of legally mandated written information electronically, provided that the consumer consents and confirms their ability to obtain the information in electronic form.

The ESIGN Act imposes several requirements, including the condition that an electronic signature is only valid when the party intends to sign. Additionally, the Act mandates that parties not only utilise electronic

[9] Miller, L., R. Lentz,A, G.(2009). Fundamentals of Business Law: Excerpted Cases. Wodsworth: Cengage Learning.

signatures and records, but also facilitate their legal use. Furthermore, the Act stipulates that the use of technology in transactions should be unbiased across federal states, and that the use of embossing devices or seals is not necessary as long as provisions for them are made in electronic means. Similar to other acts, the ESIGN Act contains exceptions. These exceptions include situations where the supply of utilities such as water or electricity has been terminated, when a court order mandates the execution of a task, and when a document is required in the handling of hazardous materials.

The statute pertains to commercial transactions between two or more entities and excludes matters related to wills, such as divorce and adoption, that are not subject to regulatory oversight. The process of signing documents electronically involves two steps: initially, the consumer must declare their permission to use paper, and then they must be informed about the electronic procedures. Furthermore, the physical acquisition of the signature. For electronic files to be reliable and accessible to all parties, it is necessary for each party to save their work on their own computers. Businesses must select an ESIGN solution that is adaptable, easily accessible, and legible.[10]

X. THE UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT

The Uniform Computer Information Transaction Act was enacted by the United States legislature to establish clear and standardised principles for regulating the transaction of computer information, including software licensing. The absence of inclusion of the software industry in the Uniform Commercial Code led to the creation of the UCITA. The National Conference of Commissioners on Uniform State Laws, in

[10] Bowman, I. (2009). Electronic Signatures in Global and National Commerce Act ("ESIGN"). Web.

partnership with the American Law Institute, introduced it in 1999 as a modification of the standardised Commercial Code to ensure consistency.

It was established in 2002. Its objective is to establish a standardised framework for regulating transactions in the field of information technology, similar to how the Uniform Commercial Code is applied in the business sector. The same statute guarantees clarity of laws pertaining to proper usage, consumer protection, shrink-wrap licenses, as well as their timing and the ability to transfer them.

Consumers are permitted to return items alone if their licenses are invalid. Not all states have accepted the Act because some believe that it does not provide sufficient security for software transactions, as there are other organisations that can not only supply protection but also develop software. This act primarily applies when computer data is utilised in a transaction. The legislation characterises computer information transaction as a legally binding agreement to create or modify computer data.

Computer information is defined as digital data that is capable of being manipulated by a computer. This legislation does not pertain to financial services, animations, or graphic programming. The first law aimed at ensuring consistency in the digital economy has been implemented, but with limited adoption. The act has achieved success primarily in Virginia and Maryland. Attempts to implement it in other jurisdictions have been unsuccessful due to disputes on its efficacy.

XI. CONCLUDING REMARKS

Owing to the notable technical progress in the contemporary world, there is a significant imperative to transition from paper-based record keeping to electronic mediums. Electronic media is also utilised for conducting business operations. The current manner of data storage and transmission lacks sufficient security measures, which leaves it

vulnerable to computer crime. This increases the danger of unauthorised alteration, modification, misuse, and ultimately the loss of a significant amount of valuable and sensitive data. The privacy of personal data is likewise susceptible to unauthorised access. These reasons have led to the implementation and implementation of the aforementioned legislation in order to protect this data.