Journal of Technology Law & Policy

Volume 20 | Issue 1 Article 2

June 2015

Crime in the Evolved Digital Age

Anar Patel (now Kanwar)

CRIME IN THE EVOLVED DIGITAL AGE

© 2015 *Anar Patel*[*]

I. INTRODUCTION

Computer technologies and the Internet present new challenges to criminal law because they offer "new ways to commit old crimes and have the means of committing crimes unknown to a pre-digital justice system."[1] "With increasing technologies available to all types of users and an array of information accessible online, including easily downloadable password cracking programs and cyber terrorism tools, the pool of potential computer criminals deepens."[2] With technology growing at an advanced rate, the numbers of computer fraud crimes have exponentially increased.[3] One of the most common forms of computer fraud is hacking, where an unauthorized individual uses technological tools to remotely access a computer through a secure network or Internet connection without authorization.[4]

In July 2005, hackers exploited security weaknesses in the local computer system of a Marshalls near St. Paul, Minnesota, and gained access to the entire TJ Maxx (TJX) network.[5] In 2007, TJX announced

---

* Anar Patel, J.D. 2015, Arizona Summit Law School; B.S. 2013, Business Administration & Management, with a concentration in Accounting, Boston University.

1. Julie A. Tower, *Hacking Vermont's Computer Crime Statute*, 25 VT. L. REV. 945, 945 (2001) (discussing how evolving computer technology is leading to more complex computer crimes). The state statutes that I am referring to are California, Vermont, Arkansas, and Arizona.

2. *Id.*

3. *Id.* at 949.

4. HG.ORG LEGAL RESOURCES, http://www.hg.org/computer-crime.html (last visited June 30, 2015).

5. Tobias Loetzke, *The TJ MAXX Credit Card Incident*, tlotzke.myweb.usf.edu/tjx_creditcard.pdf (last visited June 30, 2015).

their systems were compromised and faced the largest credit-card theft in history.[6] The company lost 45.7 million credit and debit card numbers that resulted in a large number of fraudulent transactions.[7]

There are two standards with wireless encryption: Wired Equivalent Privacy (WEP) standard and a Wi-Fi Protected Access (WPA).[8] Because WEP[9] networks were easily hacked with accessible software, the wireless industry created a better WPA[10] standard.[11] Unfortunately, TJX did not upgrade their systems to the WPA standard and hackers obtained easy access to the local system and managed to create their own user accounts with full administrator rights.[12] Not only did hackers obtain credit and debit card numbers, but also social security numbers, and driver's license numbers, which they sold in packages to private Internet pages all over the world.[13] This data was used to make fraudulent withdrawals from consumers' bank accounts.[14]

This security breach put millions of consumers at risk for identity theft and burdened banks with the financial responsibility of covering all expenses for replacing compromised cards.[15] As a result, banks lobbied for legislation to "place full financial responsibility for security breaches

---

6. Mark Jewell, *T.J. Maxx Theft Believed Largest Hack Ever*, NBC NEWS, http://www.nbcnews.com/id/17871485/ns/technology_and_science-security/t/tj-maxx-theft-believed-largest-hack-ever/ (last updated Mar. 30, 2007).

7. Loetzke, *supra* note 5.

8. Margaret Rouse, *Wi-Fi Protected Access (WPA)*, TECHTARGET (Nov. 2005), http://searchmobilecomputing.techtarget.com/definition/Wi-Fi-Protected-Access.

9. *What Is WEP Wireless Encryption?*, NETGEAR SUPPORT, http://kb.netgear.com/app/answers/detail/a_id/1141/~/what-is-wep-wireless-encryption%3F (last updated Dec. 26, 2014) ("Wired Equivalent Privacy (WEP) is a security protocol for wireless networks that encrypts transmitted data. The disadvantage is that without any security, the data can be intercepted without difficulty.").

10. Rouse, *supra* note 8.

> Wi-Fi Protected Access (WPA) is a security standard for users of computers equipped with Wi-Fi wireless connection. It is an improvement on and is expected to replace the original Wi-Fi security standard, Wired Equivalent Privacy (WEP). WPA provides more sophisticated data encryption than WEP and also provides user authentication. WEP is still considered useful for the casual home user, but insufficient for a corporate environment where the large flow of messages can enable eavesdroppers to discover encryption keys more quickly.

Id.

11. Loetzke, *supra* note 5.

12. *Id.*

13. *Id.*

14. Joseph Pereira, *How Credit-Card Data Went Out Wireless Door*, WALL ST. J., http://www.wsj.com/articles/SB117824446226991797 (last updated May 4, 2007).

15. Loetzke, *supra* note 5.

on companies whose systems are breached."[16] These new bills and regulations will force companies who fail to update their security systems to pay for resulting damages.[17] Therefore, it is of the highest importance to regularly update security systems to prevent being a target of such crimes and avoid all liabilities that could be incurred from the failure to prevent them.[18]

This Article examines computer crime[19] statutes and focuses on their weaknesses to implement statutory modifications. Part I provides an overview on the current federal statute, Computer Fraud and Abuse Act, and specific computer crime statutes from California, Vermont, Arkansas and Arizona. Part II focuses on states' approaches to computer crimes. Part III highlights potential statutory weaknesses and suggests possible amendments to federal and state legislation. Finally, Part IV of this Article concludes with a unique perspective of computer fraud, specifically hacking, in relation to financially motivated crimes.

II. COMPUTER CRIMES STATUTES

The Computer Fraud and Abuse Act, defines "fraud" and related activity in connection with computers as, "whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains (a) information contained in a financial record of a financial institution,"[20] "or of a card issuer, or contained in a file of consumer reporting agency on a consumer; (b) information from any department or agency of the United States; or information from any protected computer."[21] The federal statute focuses primarily on protecting the interests of financial institutions and the government.[22] States have enacted legislation that further defines computer related crimes and the extent to which they relate to businesses and individuals within the state.[23]

California Legislature enacted section 502 of the California Penal Code to expand the degree of protection afforded to individuals,

16. *Id.*

17. *Id.*

18. *Id.*

19. BLACK'S LAW DICTIONARY 452 (10th ed. 2014) (defining computer crime, or cybercrime, as a crime that "involves the use of a computer, such as sabotaging or stealing electronically stored data.").

20. *Id.* at 748 (defining financial institution as "[A] business, organization, or other entity that manages money, credit, or capital, such as a bank, credit union, savings-and-loan association, securities broker or dealer, pawnbroker, or investment company.").

21. 18 U.S.C. § 1030 (2008).

22. *See id.*

23. *E.g.*, CAL. PENAL CODE § 502 (2011).

businesses, and governmental agencies"[24]

> from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer system. The Legislature declared protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilizes those computers, computer systems, and data.[25]

For the purposes of this statute, "access" means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.[26]

Subdivision (b) of the statute defines the various terms used within the statute, except for the word "computer."[27] Subdivision (b)(2) defines "computer network" as "any system which provides communications between one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities."[28] Subdivision (b)(5) defines "computer system" as "a device or a collection of devices . . . , one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control."[29] Subdivision (c) of the statute is a list of "illegal activity ranging from the use of a computer to defraud or extort, to infecting a computer with a virus."[30] Subdivision (c)(7) covers one who "knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network."[31]

On September 17, 2014, an Act to amend Section 502 of the California Penal Code was filed.[32] Existing law was amended to expand the definition of computer crime, imposing a state-mandated local program.[33] This bill sought to update existing law with a heavy emphasis on disruption of government computer services or public safety

---

24. BLACK'S LAW DICTIONARY 75 (10th ed. 2014) (defining Government Agency as a governmental body with the authority to implement and administer particular legislation).

25. CAL. PENAL CODE § 502 (2011).

26. 19 CAL. JUR. 3d Criminal Law: Miscellaneous Offenses § 311 (2015).

27. People v. Lawton, 56 Cal. Rptr. 2d 521, 523 (Cal. App. Dep't. Super. Ct. 1996).

28. *Id.*

29. *Id.*

30. *Id.*

31. *Id.*

32. A.B. 1649, Cal. Gen. Assemb., Reg. Sess. (Cal. 2014).

33. *Id.*

infrastructure along with updating definitions to include newer technologies.[34] For the purposes of this statute, "access" now means "to gain entry to, instruct, cause input to, cause input from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network."[35] Subdivision (b)(2) now defines "computer network" as "any system that provides communications between one or more computer systems and input/output devices including, but not limited to, display terminals, remote systems,[36] mobile devices, and printers connected by telecommunication facilities."[37] In its effort to update the statute, the bill has fallen short. In its commendable attempts to broaden the statute to include remote systems and mobile device while providing a definition for "electronic mail," it has failed to define "computer." While it is great to include newer technologies to the statute that can be used to commit these same crimes, the bill fails to recognize the importance of defining the word "computer." If we don't know what a "computer" is or what a "computer" is capable of, how can we further understand what a "computer network," "computer system," or "computer service" is.

Vermont's computer crime statute generally prohibits four types of conduct: (1) unauthorized access; (2) access for fraudulent purposes; (3) alteration, damage, or interference; and (4) theft or destruction.[38] It bears noting that the statute casts a fairly wide net in that it protects computers, computer systems, computer networks, computer software, computer programs, and data contained in any of the foregoing.[39] Vermont's computer crime statute explains,

> a person shall not intentionally and without lawful authority access or cause to be accessed any computer, computer system, or computer network for any of the following purposes: (1) executing any scheme or artifice to defraud; (2) obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises; or (3) in connection with any scheme

34. *Id.*

35. *Id.*

36. *What Is a Remote System?*, ORACLE, http://docs.oracle.com/cd/E23824_01/html/821-1454/wwrsov-3.html (last visited Nov. 27, 2014) ("A remote system is a workstation or server that is connected to the local system with any type of physical network and configured for TCP/IP communication."); *see also* Margaret Rouse, *TCP/IP (Transmission Control Protocol/Internet Protocol) Definition*, TECHTARGET (Oct. 2008), http://searchnetworking.techtarget.com/definition/TCP-IP ("TCP/IP is short for Transmission Control Protocol/Internet Protocol and it is the basic communication language of the Internet.").

37. A.B. 1649, Cal. Gen. Assemb., Reg. Sess. (Cal. 2014).

38. Matthew S. Borick, *A Look at Vermont's Computer Crime Statute*, 34 VT. B.J. 38, 38 (2008) (citing VT. STAT. ANN. tit. 13, § 4101(2)–(7)).

39. *Id.*

or artifice to defraud, damaging, destroying, altering, deleting, copying, retrieving, interfering with or denial of access to, or removing any program or data contained therein.[40]

Under Arkansas law,

a person commits computer fraud if the person intentionally accesses or causes to be accessed [by] any computer, computer system, computer network, or any part of a computer, computer system, or computer network for the purpose of: (1) devising or executing any scheme or artifice to defraud or extort; or (2) obtaining money, property, or a service with a false or fraudulent intent, representation, or promise.[41]

Arkansas has two other statutes that define computer trespass and unlawful acts regarding computers.[42] Computer trespass is when, (3) "a person intentionally and without authorization accesses, alters, deletes, damages, destroys, or disrupts any computer, computer system, computer network, computer program or data."[43] "A person commits an unlawful act regarding a computer if the person knowingly and without authorization: . . ." (4) obtains and discloses, publishes, transfers, or uses a device used to access a computer, system, network, or data.[44]

Arizona's computer tampering statute defines,

a person who acts without authority or who exceeds authorization of use commits computer tampering by: (1) accessing, altering, damaging or destroying any computer, computer system or network, or any part of a computer, computer system or network, with the intent to devise or execute any scheme or artifice to defraud or deceive, or to control property or services by means of false or fraudulent pretenses, representations or promises; (2) knowingly altering, damaging, or destroying computer programs or data; (3) knowingly introducing a computer contaminant into any computer, computer system or network; (4) recklessly disrupting or causing the disruption of computer, computer system or network services or denying or causing the denial of computer network services to any authorized user of a computer, computer system or network; (5) recklessly using a computer, computer system or network to engage in an scheme or course of conduct

40. VT. STAT. ANN. tit. 13, § 4103 (West 1999).
41. ARK. CODE § 5-41-103 (1987).
42. ARK. CODE § 5-41-104 (1987); ARK. CODE § 5-41-202 (2007).
43. ARK. CODE § 5-41-104 (1987).
44. ARK. CODE § 5-41-202 (2007).

> that is directed at another person and that seriously alarms, torments, threatens or terrorizes the person . . . ; (6) preventing a computer user from exiting a site, computer system or network-connected location in order to compel the user's computer to continue communicating with, connecting to or displaying the content of the service, site or system; (7) knowingly obtaining any information that is required by law to be kept confidential or any records that are not public records by accessing any computer, computer system or network that is operated by this state . . . ; and (8) knowingly accessing any computer, computer system or network or any computer software, program or data that is contained in a computer, computer system or network.[45]

Arizona's computer tampering statute not only provides a broad definition of acts considered as computer tampering, but also provides a guideline for which counties a prosecution for a violation of this section may be tried in.[46]

III. STATUTORY APPROACH

The evolving nature of the Internet makes it difficult for the United States to "develop and implement electronic criminal and civil laws that protect Americans."[47] Computer fraud and cyberattacks become more advanced with each day while the federal government continues to fight cybercrime with an outdated federal statute.[48] The increased use of computers has been accompanied by an increase in computer fraud and computer related crimes.[49] The Computer Fraud and Abuse Act (CFAA) is a federal computer security statute that aims to protect computers operated by financial institutions, the federal government, and computers linked to the Internet.[50] For years, courts have taken two approaches interpreting the terms of the CFAA.[51] "Courts around the country struggle with whether the CFAA applies in a situation where an employee who

---

45. ARIZ. REV. STAT. § 13-2316 (2011).

46. *See id.*

47. W. Cagney McCormick, *The Computer Fraud & Abuse Act: Failing to Evolve with the Digital Age*, 16 SMU SCI. & TECH. L. REV. 481, 481 (2013).

48. *Id.*

49. Steven Damian Imparl, *Validity, Construction, and Application of State Computer Crime and Fraud Laws*, 87 A.L.R. 6th 1, 1 (2013).

50. Fernando M. Pinguelo & Bradford W. Muller, *Virtual Crimes, Real Damages: A Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminals*, 16 VA. J.L. & TECH. 116, 139 (2011).

51. Cranel, Inc. v. Pro Image Consultants Grp. LLC, No. 2:13-CV-766, 2014 WL 4829485, at *5 (S.D. Ohio Sept. 29, 2014).

has been granted access to his employer's computers uses that access for an improper purpose."[52] A court that has adopted the narrow approach held that, "once an employee is granted 'authorization' to access an employer's computer that stores confidential company information, the employee does not violate the CFAA regardless of how he subsequently uses the information."[53] Another court that adopted the broader approach held that, "an employee access[es] a computer without authorization when the employee, without the employer's knowledge, acquires an interest that is adverse to that of his employer or is guilty of a serious breach of loyalty."[54] While many courts argue that the CFAA's plain language and legislative history support the narrow approach, and adopting the narrow approach rules out any ambiguity,[55] the fact that courts have argued for both the narrow and the broad approach prove ambiguity exists. As the federal statute is ambiguous and outdated, states have enacted legislation defining aspects of computer fraud.[56]

"All fifty states have enacted legislation that may impact a user's access to open wireless networks."[57] These statutes vary in name, including: "computer trespass, unauthorized use, computer tampering, computer crime, criminal use of a computer, offenses against computer users, and criminal invasion of computer privacy."[58] A substantial number of states outlaw using computers to commit fraud, or using a "computer, computer system, computer network, or any part thereof for the purpose of devising, or executing any scheme or artifice to defraud,"[59] or for "obtaining money, property, or services by means of false or

52. *Id.*

53. *Id.*

54. *Id.*

55. Shurguard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000); *see also* S. Rep. No. 99-432 (1986) (explaining that the first version of the CFAA was passed in 1984, and this first bill was directed at protecting classified information on government computers as well as protecting financial records and credit information on government and financial institution computers. In 1986, the CFAA was amended to "provide additional penalties for fraud and related activities in connection with access devices and computers." Specifically, the 1986 amendments added protection for "federal interest computers," and therefore, the original version of the CFAA did not intend to enact sweeping federal jurisdiction.).

56. Imparl, *supra* note 49, at 18.

57. Matthew Bierlein, *Policing The Wireless World: Access Liability In The Open Wi-Fi Era*, 67 OHIO ST. L.J. 1123, 1136 (2006).

58. *Id.* at 1136–37.

59. 2 Data Sec. & Privacy Law § 15:25 (2014); Pinguelo, 16 VA. J.L. & TECH. at 132 (explaining that hacking is an example of using computers to commit fraud. Hacking is defined as "gaining unauthorized access to a computer system, programs or data." Hackers sometimes hack into government networks or business networks for profit among other things. Hackers can now easily retrieve an attack code from the Internet and use it against victim websites without leaving a trace.).

fraudulent pretenses, representations, or promises."[60] A substantial "number of states have adopted 'identity theft' or 'identity fraud' statutes, which make it a crime to 'knowingly and with intent to defraud for economic benefit' obtain, possess, transfer, use, or attempt 'to obtain, possess, transfer or use, one or more identification documents or personal identification number of another person.'"[61] A majority of states have defined at least one form of unauthorized access to a computer or the data contained therein as criminal.[62] The federal computer crime law parallels this treatment of access.[63] These statutes define access to mean, "to instruct, communicate with, store data in or retrieve data from a computer, computer system, or computer network."[64] "Criminal liability attaches without regard to the defendant's further intent with respect to the purpose of the unauthorized access, but most statutes require intent or knowledge to commit the unauthorized access itself."[65] "State statutes vary with regard to the mens rea and scope of the offense."[66]

The California Penal Code § 502 defines unauthorized access to computers, computer systems, and computer data.[67] In *People v. Lawton*, the defendant was convicted of unauthorized access to a computer system, and appealed, contending that subdivision (c)(7)[68] of the California Penal Code § 502 covers only unauthorized access of *hardware*.[69] *People v. Lawton* paraphrases the statute to read that a "computer system" is a functioning combination of hardware[70] and software,[71] and a "computer network" is the hardware and software which links one or more systems with each other and with terminals and

60. 2 Data Sec. & Privacy Law § 15:25 (2014).

61. *Id.*

62. Law of Computer Technology § 18:19.

63. *Id.*

64. *Id.*

65. *Id.*

66. Bierlein, *supra* note 57, at 1137.

67. CAL. PENAL CODE § 502 (2011).

68. *Id.* (defining California Penal Code § 502, subdivision (c)(7) as any person that "knowingly and without permission accesses or causes to be accessed by any computer, computer system or computer network," is guilty of a public offense.).

69. People v. Lawton, 56 Cal. Rptr. 2d 521, 523 (Cal. App. Dep't. Super. Ct. 1996).

70. Tim Fisher, *Hardware (Computer Hardware)*, ABOUT TECHNOLOGY, http://pcsupport.about.com/od/termshm/g/hardware.htm (last visited Nov. 27, 2014) ("Computer hardware refers to the physical components that make up a computer system. There are many different kinds of hardware that can be installed inside, and connected to the outside, of a computer.").

71. *Computer Software Definition*, OPENPROJECTS, http://www.openprojects.org/software-definition.htm (last visited Nov. 27, 2014) ("Software is a term used for organized collections of computer data and instructions, often broken down into two major categories: system software and application software. System software is responsible for controlling, integrating, and managing the individual hardware components of a computer system. Application software is used to accomplish specific tasks.").

printers.[72] In other words, the California appellate court interprets both "computer system" and "computer network" as consisting of hardware and software.[73] Based on this, the court rejects the Appellant's contention and explains such interpretation, that § 502 covers only unauthorized access of hardware, would clash with the overall statutory intent to comprehensively protect the integrity of private, commercial and governmental computer systems and data.[74] Upon review of various provisions of Penal Code § 502, subdivision (c) reveals that adopting the Appellant's argument would carve a loophole in the statute that was not intended by its drafters.[75] Because public access computer terminals are increasingly common in the offices of many governmental bodies and agencies, the Court determines subdivision (c)(7) was designed to criminalize unauthorized access to software and data in such systems.[76]

In response to the new variety of computer crime, the Vermont General Assembly enacted a computer crime statue in May 1999, An Act Relating to Computer Crimes.[77] Vermont's law makes certain acts involving computers illegal including, "knowingly accessing any computer system or data without permission; accessing a computer to commit fraud; intentionally altering, damaging or interfering with another system; stealing information from computer systems, or depriving an owner access to their system."[78] In 2000, the General Assembly enacted "An Act Related to Internet Crimes," which revised existing criminal laws to make clear that they apply in situations where the crime is committed through the use of the Internet, or by use of a computer or other electronic communication device.[79] "The need for state[-level] computer crime legislation naturally fits with increasing Internet dependence, escalating electronic commerce, and growing interest in maintaining privacy of personal information."[80] Computer crime laws give police and prosecutors the necessary tools to address criminal behaviors initiated by computer technologies and permits law enforcement to apprehend computer criminals.[81]

As most businesses and the government in Vermont could not survive without properly functioning computers that manage and store crucial information, the statute is necessary to protect the information and

72. *Lawton*, 56 Cal. Rptr. 2d at 523.
73. *Id.*
74. *Id.*
75. *Id.*
76. *Id.*
77. Tower, *supra* note 1, at 945.
78. *Id.* at 945–46.
79. *Id.* at 946.
80. *Id.* at 947–48.
81. *Id.* at 948.

services that computers store and provide.[82]

Vermont's computer crime statute, "An Act Relating to Computer Crimes," criminalized computer-related activities in an attempt to get tough on cybercriminals.[83] However, the statute is in need of legislative reform in order to effectively prosecute computer crimes.[84] While Vermont's statute conveys conciseness and clarity, it falls short of serving as an effective vehicle for prosecuting computer crimes.[85] Section 4101 of "An Act Relating to Computer Crimes" is a glossary that defines computer-related terms used throughout the statute.[86] Section 4102 deals with unauthorized access of any computer, computer system, computer network, computer program or data.[87] Section 4103 makes it a crime to access computers for fraudulent purposes.[88] Section 4104 addresses alteration, damage, or interference with the operation of any computer, computer system, computer network, computer software, computer program, or data.[89] Section 4105 criminalizes the theft or destruction of a computer system, computer network, computer software, computer program, or data.[90] Section 4106 addresses civil liability and permits a person damaged as a result of a violation of the statute to bring civil action against the violator.[91] Lastly, section 4107 pertains to venue, and provides that any violation of the statute shall be considered to have been committed in the state, if Vermont is the state from which or to which any use of a computer or computer network was made.[92]

While legislators attempted to balance the need to devise statutory language that is broad enough to yield an effective prosecution and constitutional rights, Vermont's computer crimes statute illustrates where such attempts can fall short, which amounts to something that is less than effective legislation.[93] Specifically, Vermont's computer crime statute contains several inadequacies or loopholes where language is too broad or highly generalized, when it could be more specific and detailed.[94] Additionally, this new but outdated statute is steps behind technology and therefore demands review to promote effective prosecution of computer

82. *Id.* at 949.
83. *Id.* at 957.
84. *Id.* at 958.
85. *Id.* at 961.
86. *Id.* at 958–59 (citing VT. STAT. ANN. tit. 13, § 4101).
87. *Id.* at 959.
88. *Id.* (citing VT. STAT. ANN. tit. 13, § 4102).
89. *Id.* (citing VT. STAT. tit. 13, § 4104).
90. *Id.* (citing VT. STAT. ANN. tit. 13, § 4105).
91. *Id.* (citing VT. STAT. ANN. tit. 13, § 4106).
92. *Id.* (citing VT. STAT. ANN. tit. 13, § 4107).
93. *Id.* at 961.
94. *Id.*

crimes.[95] Section 4103, "Access to Computer for Fraudulent Purposes," raises several definitional concerns that should be addressed.[96] This section of Vermont's computer crimes statute does not define who is a "person" and what constitutes "without lawful authority."[97] Ambiguous and undefined terminology makes the statute unenforceable, therefore obstructing effective prosecution of such crimes.[98]

Arkansas enacted a broad range of computer crime statutes, and the two statutes most applicable to businesses are computer trespass and computer fraud.[99] Computer trespass occurs when a person alters or damages any computer, computer system, network, program or data.[100] Computer fraud occurs when a person accesses a computer, computer system, or computer network to defraud, extort or fraudulently obtain property.[101] No reported discussions exist discussing the Arkansas computer crime statutes, but these laws will prove quite valuable to firms in the future to protect their valuable business information.[102]

Arizona Statute § 13-2316 defines various behaviors and acts that amount to computer tampering.[103] In *State v. Fimbres*, the appellant, Javier Fimbres, was convicted of three counts of computer tampering along with other criminal charges, which he appealed by arguing the State presented insufficient evidence to support several of his convictions.[104] The appellant purchased merchandise from local stores using gift cards that were altered so that the information encoded in the magnetic strips on the back of the cards corresponded with various credit and debit card numbers.[105] These credit and debit cards did not belong to the appellant, and he did not have permission to use the cards or access the underlying accounts.[106] During several transactions, the appellant presented other cards that were declined before presenting a card that was accepted.[107] After the appellant was apprehended and the case went to trial, the State presented evidence that unauthorized transactions had been made on several victims' credit cards and debit accounts.[108] Surveillance cameras

95. *Id.*
96. *Id.* at 967.
97. *Id.*
98. *See id.* at 966.
99. Kevin M. Lemley, *Beyond Trade Secrets: Protecting Business Information in Arkansas*, 43 SPG ARK. LAW. 10, 13 (2008).
100. *Id.* (citing ARK. CODE ANN. § 5-41-104).
101. *Id.* (citing ARK. CODE ANN. § 5-41-103).
102. *Id.*
103. *See* ARIZ. REV. STAT. ANN. § 13-2316 (2014).
104. State v. Fimbres, 213 P.3d 1020, 1023 (2009).
105. *Id.*
106. *Id.*
107. *Id.*
108. *Id.*

from the store also showed the appellant using the gift cards to pay for merchandise.[109] While the appellant admitted he made purchases with the gift cards, he claimed that he did not know that the cards had been altered.[110]

Appellant claimed that the evidence presented against him could not support a computer tampering conviction because the plain meaning of § 13-2316 demonstrated the statute was enacted solely to criminalize "computer hacking" and does not include other computer-related conduct, such as swiping gift cards encoded with illegally obtained credit and debit card numbers through a credit card reader.[111] The court determined that the plain meaning of § 13-2316 is clear and demonstrated the statute is not limited to computer hacking.[112] A.R.S § 13-2316 provides:

> A person who acts without authority or who exceeds authorization of use commits computer tampering by . . . accessing, altering, damaging or destroying any computer, computer system or network, or any part of a computer, computer system or network, with the intent to devise or execute any scheme or artifice to defraud or deceive, or to control property or services by means "accessing" a computer system with the intent to defraud is a far broader prohibition than "computer hacking," and the appellant's actions here fall within that prohibition.[113]

The court further found that in order for a store's credit card reader to charge or debit customers' accounts, the reader must be linked to the store's computer system or network.[114] Therefore, the court concluded a defendant who swipes gift cards bearing illegally obtained credit and debit card numbers in a store credit card reader ultimately accesses the store's computer system or network with the intent to execute a scheme to defraud.[115]

Another application of A.R.S. § 13-2316 is demonstrated in *State v. Young*, where the defendant, Clifton Young, was convicted of computer tampering in violation of § 13-2316(A)(7).[116] The defendant was employed by the Arizona Department of Transportation (ADOT) as a member of the server management team.[117] As a member of the team, the

109. *Id.*
110. *Id.* at 1023–24.
111. *Id.* at 1025.
112. *Id.*
113. *Id.* (citing Ariz. Rev. Stat. Ann. § 13-2316).
114. *Id.*
115. *Id.* at 1023.
116. *Young*, 224 P.3d 944, 946 (Ariz. Ct. App. 2010).
117. *Id.*

defendant had elevated domain administrator privileges that provided him with access to all computer servers on the ADOT computer networks.[118] Among the servers on the ADOT network was one that hosted the personnel files of ADOT employees.[119] ADOT employees are subject to annual reviews of their work performance and as part of the review process, employees are given an Employee Performance Appraisal System (EPAS) score.[120] In 2006, the Chief Information Officer at ADOT decided that the EPAS scores in the IT department had become inflated over the years and directed the department managers to recalibrate the scores to establish a more realistic scoring baseline, which subsequently reduced the scores.[121] The defendant showed another member of the team an Excel spreadsheet displayed on a computer in his cubicle that included names and EPAS scores for the entire IT department and the information on the spreadsheet indicated that the server management team was the only group in the IT department to have its EPAS scores lowered.[122] The defendant informed a supervisor of this observation to which the supervisor said he would take the spreadsheet to his superior.[123] After the supervisor spoke to his superior, ADOT began an internal investigation to discover the source of the unauthorized disclosure of the EPAS scores and through forensic examination found the EPAS spreadsheet was accessed from the defendant's computer using his user ID and password.[124] After the discovery, the defendant was terminated from his position and charged with computer tampering in violation of A.R.S. § 13-2316(A)(7) of which he was convicted.[125]

On appeal, the defendant argued that the evidence presented at trial was insufficient to support his conviction.[126] A.R.S. § 13-2316(A)(7) provides:

> A person who acts without authority or who exceeds authorization of use commits computer tampering by: (7) knowingly obtaining any information that is required by law to be kept confidential or any records that are not public records by accessing any computer, computer system or network that is operated by this state, a political subdivision of this state or a medical institution.[127]

---

118. *Id.*
119. *Id.*
120. *Id.*
121. *Id.*
122. *Id.*
123. *Id.*
124. *Id.* at 946–47.
125. *Id.* at 947.
126. *Id.* at 946.
127. *Id.* at 947.

The court determined that the evidence presented at trial was sufficient to show that the defendant acted without authority when he accessed certain data on a government computer, but the statute's description of "records that are not public records" unambiguously refers to records that do not fall within the public records law—not merely to records that might be exempt from disclosure under the public records law.[128] The court concluded that because the data that the defendant obtained is subject to the public records law, there was insufficient evidence that the defendant obtained the type of information described by the plain language of the subsection under which he was charged.[129]

IV. COMBATING COMPUTER FRAUD

The Computer Fraud and Abuse Act affords the broadest protection against computer crimes, but it is not very specific. To accompany the broad, ambiguous language of the federal statute, states have enacted legislation to combat computer crime that is much stricter than the federal statute. Both the federal statute and state statutes protect against unauthorized access of a computer, computer system, computer network, computer program or data,[130] but neither the federal statute nor the state statutes are updated to include mobile devices such as smartphones[131] or tablet computers[132] in the working definition of "computer."[133] These outdated statutes need to be updated to include "any electronic or digital

128. *Id.* at 946.

129. *Id.*

130. 18 U.S.C. § 1030 (2014);

131. *Smartphone*, PC MAG, http://www.pcmag.com/encyclopedia/term/51537/smartphone (last visited Nov. 28, 2014) (A smartphone is a cellphone and handheld computer in one. A smartphone can do everything a personal computer can do, and because of the GPS feature a smartphone can do much more. A smartphone combines cellular telephone, Internet access for e-mail and Web, music and movie player, camera and camcorder, GPS navigation system and a voice search for asking a question about anything.).

132. Margaret Rouse, *Tablet (Tablet PC) Definition*, TECHTARGET (July 2014), http://searchmobilecomputing.techtarget.com/definition/tablet-PC ("A tablet [computer] is a wireless, portable personal computer with a touch screen interface. The tablet . . . is typically smaller than a notebook computer, but larger than a smartphone. Technological advances [to] battery life, display resolution, handwriting recognition software, memory, and wireless Internet access have made . . . tablets a viable computer option" and with added keyboard and mouse accessories, the tablet can serve to replace typical personal computers.).

133. 18 U.S.C. § 1030(e)(1) (2014).

device[134] that is transmittal or can be transmitted,"[135] rather than "computer, computer systems, computer networks." Mobile devices, or any other electronic or digital devices, can be considered a "computer," or "computer system" because, as users, we can use and access the same important information via email, social media, and mobile applications from financial institutes, as we would on our personal or business computers. Anyone can hack into smartphones or tablets, or any other transmittal electronic devices and retrieve sensitive information that can lead to identity theft for monetary gain.

To avoid mishaps such as the TJX incident, the federal statute needs to hold businesses liable for securing its own data. The federal statute needs to mandate businesses, financial institutions, and the government to have a two-factor[136] or multifactor authentication[137] rather than single-

134. DEL. CODE tit. 12, § 5002 (2015) ("[A] 'digital device' [is] an electronic device that can create, generate, send, share, communicate, receive, store, display, or process information, and such electronic devices shall include, but not limited to, desktops, laptops, tablets, peripherals, servers, mobile telephones, smartphones, and any similar storage device which currently exists or may exist as technology develops or such comparable items as technology develops.").

135. 19 U.S.C. § 1401 (2014) (explaining that an electronic or digital device that is transmitted creates an electronic transmission. Electronic transmission means "the transfer of data or information through an authorized electronic data interchange system consisting of, but not limited to, computer modems and computer networks.").

136. Margaret Rouse, *Two-Factor Authentication (2FA)*, SEARCHSECURITY (Mar. 2015), http://searchsecurity.techtarget.com/definition/ two-factor-authentication.

> Two-factor authentication is a security process in which the user provides two means of identification, . . . a physical token . . . and . . . something that is typically memorized . . . . A[n] . . . example of [such] authentication is a bankcard: the card . . . is the physical item[,] and the personal identification number (PIN) is the data that [correlates to the bankcard] . . . . [T]wo-factor authentication [could] drastically reduce the incidence of online identity theft, phishing expeditions, and other online fraud, because the victim's password [would no longer be enough] to give [the] thief access to their information.

Id.

137. Margaret Rouse, *Multifactor Authentication (MFA)*, SEARCHSECURITY (Mar. 2015), http://searchsecurity.techtarget.com/definition/ multifactor-authentication-MFA.

> Multifactor authentication (MFA) is a security system that requires more than one [form] of authentication . . . to verify the [legitimacy of a transaction]. Multifactor authentication combines two or more independent credentials . . . [involving the possession of a physical token and a password, which is used in conjunction with biometric data]. The goal of MFA is to create a layered defense [to] make it more difficult for an unauthorized person to gain access to a target such as a physical location, computing device, network of database. If one factor [were] compromised . . . , [then] the attacker [would have to get through] at least one more barrier to breach before successfully breaking into the target.

Id.

factor authentication[138] for passwords and other sensitive information. Businesses often provide employees with company phones, tablets, or laptops. Anyone with the right means can get a hold of, and/or hack into any single employee's company phone or tablet and retrieve sensitive company information. Hackers can use the sensitive company information by gaining unauthorized access to an employee's company phone or tablet, and use this information to fraudulently gain access to the business's entire system or network. This is why it is important to have two-factor or multifactor authentication to protect the company's sensitive information.

With increased use of cell phones and tablets, more mobile applications,[139] which are linked to web user accounts,[140] are being created. While these applications may be secure due to added safeguards to protect customer information, the web user accounts created to use with these applications may not be secure. For example, we may download applications such as the Starbucks App, which allows payment for Starbucks items by scanning the barcode from a smartphone. There is no more hassle of pulling out your wallet and holding up the line behind you. By simply accessing the app, and touching "pay" you are ready to be checked out to wait for your delicious Starbucks item. Another convenient feature of the app allows you to store credit card information to the Starbucks Account you created, which can accessed on the phone/tablet application and the web, to reload money on to your Starbucks Rewards Card quickly and easily. While the credit card information is secure on the application, hackers have gained access into the Starbucks web user accounts and reloaded Starbucks Rewards Cards for upwards of $200 in $100 increments using the credit cards on file. By linking their Rewards card to a user account, hackers then transfer the

---

138. Margaret Rouse, *Single-Factor Authentication (SFA)*, SEARCHSECURITY (Mar. 2015), http://searchsecurity.techtarget.com/definition/single-factor-authentication-SFA.

> Single-factor authentication (SFA) is the traditional security process that requires a user name and password before granting access to the user. [SFA] relies on the diligence of the . . . user[,] who [should take additional precautions such as] creating a strong password and ensuring no [other individual] can access it.

Id.

139. Priya Viswanathan, *What is a Mobile Application?*, ABOUT TECH, http://mobiledevices.about.com/od/glossary/g/What-Is-A-Mobile-Application.htm. ("Mobile applications or mobile apps are [software] applications [designed to run on] small handheld devices, such as mobile phones, smartphones, PDAs[, tablet computer.]").

140. *User Account*, PC MAG, http://www.pcmag.com/encyclopedia/term/53549/user-account (last visited Nov. 29, 2014) ("[A user account is] an established relationship between a user and a computer, network[,] or information service. User accounts are assigned a username [and passwords, while] optional for computers and networks, [are] mandatory for registrations and subscriptions to online services.").

reloaded amount from the user's Starbucks Rewards Card to theirs. Hackers then delete all the Rewards cards associated with the user's account to erase any trace, leaving no way to track the thief or the money.

As careful as we may be with technology and our personal information, we sometimes forget to ask what security measures are taken to protect our identity and information in the name of convenience. When such incidents occur, Starbucks claims, "[they] believe [the] customer's log-in credentials were compromised, likely due to weak password conventions."[141] While this may be true, it is not entirely the customer's fault. Because Starbucks never required the customer to use more secure passwords in the first place, how can Starbucks expect customers to have strong password conventions?

Companies with such applications, where loyalty cards and/or credit cards are linked to the user's web account, should impose secure password requirements when signing up for the account. Furthermore, for current users, companies can change the terms and conditions[142] to update passwords per the secure password requirements. That way the next time a user tries to log into his/her account, he/she must update his/her password to meet the secure password requirements. To impose secure password requirements, the company can require users to create passwords that include: 8 characters, 1 lowercase letter, 1 uppercase letter, and 1 symbol. While it is important to impose secure password requirements in the first place, it is also important to understand that having a secure password alone does not ensure security to any account. In order to truly have a secure account, the secure password must be accompanied by another security measure. Just having one of those security measures leaves the account vulnerable. However, having two security measures makes gaining unauthorized access to the accounts less likely. While there are no guarantees that an account cannot be hacked, adding layers of security measures makes the account less penetrable to hackers by creating more walls to breach in order to gain unauthorized

---

141. Bruce Erskine, *Starbucks Blames Weak Password for Phone App Hacking*, CHRON. HERALD (July 8, 2014, 4:32 PM), http://thechronicleherald.ca/business/1221352-starbucks-blames-weak-password-for-phone-app-hacking.

142. Cory Janssen, *Clickwrap Agreement*, TECHOPEDIA, http://www.techopedia.com/definition/4243/clickwrap-agreement (last visited Nov. 27, 2014).

> A clickwrap agreement is a type of contract that is widely used with software licenses and online transactions in which a user must agree to terms and conditions prior to using the product or service. . . . [M]ost clickwrap agreements require the consent of end users by clicking . . . "I Accept" or "I Agree" button . . . [in] a dialog box. [If t]he user . . . reject[s] the agreement[,] . . . the user . . . [is] unable to use the service or product.

Id.

access.

It is imperative that businesses are up to date with all security measures and take extra measures to ensure the customer's safety. In the TJX incident, TJX did not upgrade their Wi-Fi standard to WPA. Due to TJX's failure to upgrade to the more secure Wi-Fi standard, hackers were easily able to gain access to sensitive information and data stored on TJX's systems. As a result, hackers were able to change system administrator settings[143] within the system to give themselves complete access to all sensitive data.

Businesses should be required to take preventive measures to protect themselves and the identities of their customers from such incidents. Businesses have a moral obligation to their clients, consumers, or customers to protect their identity. If businesses are not taking proper precautions and fail to implement the latest security standard, businesses are compromising consumer identity and opening themselves up to a variety of lawsuits. The federal statute serves to combat computer crimes, but attacks, such as the TJX incident, are still occurring because businesses are not updating their security. In order to protect against computer crimes, businesses should be constantly updating security to the latest security standards in efforts toward taking preventive measures. However, businesses are not taking such preventive measure, and therefore it is imperative the federal statute mandate these businesses to constantly update their security to the latest standard in order to reduce the level of risk.

V. CONCLUSION

Due to the rapidly evolving nature of technology, legislation must keep pace with cybercrime. Although state statues have shown improvement over the federal statue, both still need refinement to reflect current times and technology. Fraud and identity theft existed before

---

143. Margaret Rouse, *System Administrator*, SEARCHNETWORKING (July 2007), http://searchnetworking.techtarget.com/definition/system-administrator.

> There are two types of administrators: a systems administrator and a network administrator. A system administrator . . . is a person who is responsible for managing a multi-user computing environment . . . by installing and configuring system hardware and software, establishing and managing user accounts, upgrading software and backup and recovery tasks.

Id.; *see also Network Administrator*, TECHOPEDIA, http://www.techo pedia.com/definition/8548/network-administrator (last visited Nov. 27, 2014) ("A network administrator is an IT expert who manages an organization's network . . . [by] installing, maintaining and upgrading any software or hardware required to efficiently run a computer network.").

computers, but with technological advancements like the Internet, crime has now become more sophisticated. Computer criminals now use computers and computer-like devices to hack into personal and business files to retrieve sensitive data. This sensitive data is used to make fraudulent bank transactions, undermine an entire business, or worse. Although it may be impossible for legislation to be one-step ahead due to the nature of technological advancement, it is possible to update statutes to encompass all devices that may be used to commit computer crimes and take preventive measures against such crimes.