VIRGINIA JOURNAL OF LAW & TECHNOLOGY

SPRING 2011 UNIVERSITY OF VIRGINIA VOL. 16, NO. 01

Virtual Crimes, Real Damages: *A Primer On Cybercrimes In The United States and Efforts to Combat Cybercriminals*

FERNANDO M. PINGUELO AND BRADFORD W. MULLER[†]

ABSTRACT

A dangerous aspect of the Internet Age that all businesses and government agencies must effectively counteract is cybercrime. As technology advances, so do the criminals. Recent media coverage of the attacks on corporate websites in response to the lockdown on WikiLeaks and its founder has renewed public focus on the vulnerabilities of corporate IT security and the profile of cybercriminals. While the recent cyber strikes on Amazon, PayPal, and MasterCard may not have been as debilitating as some other more elaborate schemes, the assaults demonstrate how quickly a group of loosely affiliated hackers can mobilize behind a cause – or in the case of Julian Assange, a martyr – and bring about significant inconvenience, if not considerable damage. This article provides a brief overview of the current status of state and federal law and enforcement activities pertaining cybercrime and the cybercriminal.

TABLE OF CONTENTS

I. INTRODUCTION

¶ 1 A dangerous aspect of the Internet Age that all businesses and government agencies must effectively counteract is cybercrime. As technology advances, so do the criminals. Recent media coverage of the attacks on corporate websites in response to the lockdown on WikiLeaks and its founder has renewed public focus on the vulnerabilities of corporate IT security and the profile of cybercriminals.[1] While the recent cyber strikes

*A working version of this article was presented at the Second Congress on Electronic Crimes and Forms of Protection, September 28, 2010, São Paulo, Brazil.

† Fernando M. Pinguelo, a Partner at Norris, McLaughlin & Marcus, P.A. and co-Chair of the Response to Electronic Discovery & Information Group at the firm, is a United States-based trial lawyer who devotes his law practice to complex business lawsuits with an emphasis on how technology impacts them. He has lectured internationally and written dozens of articles on the topic; and appeared on television as a legal commentator on various high-profile cases. He works closely with business owners and executives to develop strategies to manage business and legal issues related to electronic documents. As an adjunct professor at Seton Hall University School of Law, Mr. Pinguelo has developed and teaches a state-of-the-art course on eDiscovery and how technology impacts lawsuits. Recently, the U.S. Fulbright Program designated him a Fulbright Specialist for his work in eDiscovery; and he will guest lecture at Mackenzie University, São Paulo, Brazil next year. Finally, Mr. Pinguelo also founded and contributes to the *ABA Journal* award-winning blog, eLessons Learned – Where Law, Technology, & Human Error Collide. To learn more about Mr. Pinguelo, visit www.NJLocalLaw.com or email him at info@NJLocalLaw.com.

Bradford W. Muller, an Associate at Norris, McLaughlin & Marcus, P.A., and a member of the firm's Litigation and Internet Law groups, is a graduate of Seton Hall University School of Law, *magna cum laude*, where he was a Comments Editor on the *Seton Hall Law Review*. Prior to his current position, Mr.

on Amazon, PayPal, and MasterCard may not have been as debilitating as some other more elaborate schemes, the assaults demonstrate how quickly a group of loosely affiliated hackers can mobilize behind a cause – or in the case of Julian Assange, a martyr – and bring about significant inconvenience, if not considerable damage.[2]

¶ 2 For American businesses, and government at the federal and state levels, the potential cost of these attacks is staggering. President Obama has made the stakes clear, arguing that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and "America's economic prosperity in the 21st century will depend on cybersecurity."[3] In this article, we endeavor to explain what cybercrimes are, profile the cybercriminal, provide a discussion of some of the most common forms of cybercrimes effecting American businesses and the federal and state governments today, and discuss action that the government and businesses are taking to fight back.

¶ 3 "Cybercrime," an amorphous term that, at its greatest breadth, is used to describe "any crime that is facilitated or committed using a computer, network, or hardware device,"[4] began to catch mainstream attention in the 1980s, when "[t]he public and scientific view of computer crime radically changed . . . [after the] press published astonishing cases about hacking, viruses and worms."[5] Later in the decade, facing increased public pressure, Congress passed the Computer Fraud and Abuse Act ("CFAA"), which outlawed such things as hacking into a government computer.[6] Public

---

Muller was a Judicial Law Clerk to the Honorable Anthony J. Parrillo, New Jersey Superior Court, Appellate Division.

[1] *See* Gautham Nagesh, *Hackers Attack Mastercard, Paypal over WikiLeaks*, THE HILL, Dec. 8. 2010, http://thehill.com/blogs/hillicon-valley/technology/132751-hackers-attack-mastercard-paypal-over-wikileaks.

[2] *Id.* These problems are made even more pressing by the fact that the number of cyber-attacks is growing exponentially, and much of the nation's, indeed the world's, critical infrastructure remains vulnerable to attack. *See* Stewart Baker, Natalia Filipiak, Katrina Timlin, *In the Dark: Crucial Industries Confront Cyberattacks* (2011), *available at* http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf.

[3] Barack Obama, U.S. President, Remarks by the President on Securing our Nation's Cyber Infrastructure (May 29, 2009), http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

[4] Sarah Gordon & Richard Ford, *On the Definition and Classification of Cybercrime*, 2 J. COMPUTER VIROLOGY 13, 14 (2006), *available at* http://www.springerlink.com/content/e370t47k73321114/fulltext.pdf. "There is no generally accepted precise definition of 'cybercrime.' The activity can consist of traditional crimes (fraud, theft, extortion) or 'new' types of criminal activity (denial of service attacks, malware)." Susan W. Brenner & Leo L. Clarke, *Distributed Security: Preventing Cybercrime*, 23 J. MARSHALL J. COMPUTER & INFO. L. 659, 665–66 (2005).

[5] Ulrich Sieber, Legal Aspects of Computer-Related Crime in the Information Society (1998), http://www.archividelnovecento.it/archivinovecento/CAPPATO/Cappato/Faldone64-12Dirittiumanipaesiextracom/DonneAfghanistan/Desktop/sieber.pdf; Randy James, *A Brief History of Cybercrime*, TIME, June 1, 2009, *available at* http://www.time.com/time/nation/article/0,8599,1902073,00.html.

[6] 18 U.S.C. § 1030 (2010). The CFA "protects computers in which there is a federal interest—federal computers, bank computers, and computers used in or effecting interstate and foreign commerce. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. It is not a comprehensive provision; instead it fills cracks and gaps in the protection afforded by other state and federal criminal laws." CHARLES DOYLE, CONG. RESEARCH SERV., CYBERCRIME: AN OVERVIEW OF

awareness regarding cybercrime grew exponentially in the late 1990s and early 2000s thanks to the explosive growth in Internet usage and the "Melissa" and "I Love You"[7] viruses, which sparked the sale of virus and worm protection software.[8] The rise of "spam" email messages then lead to the passage of the CAN-SPAM Act,[9] a federal law that attempts to govern this insidious variety of unsolicited commercial messages. [10] Today, cybercrime has become so profitable and widespread that it makes earlier cases resemble child's play.

¶ 4 The complexities of the cyber schemes have proven dynamic, evolving to meet the increased security measures employed by both business and government. Attacks on businesses include such things as the theft of intellectual property, seizing bank accounts,[11] generating and distributing malware,[12] and other disruptive activity.[13] Cyber attacks against the federal government can have an even greater negative impact, potentially devastating the country's digital infrastructure or leading to the exposure of highly classified information.[14] Perhaps most disturbing is that terrorist groups have

---

THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS 1 (2010), *available at* http://www.fas.org/sgp/crs/misc/97-1025.pdf.

[7] "The ILOVEYOU virus and variants . . . was estimated to have hit millions of users and cost billions of dollars in damage." Mohammad Iqbal, *Defining Cyberterrorism*, 22 J. MARSHALL J. COMPUTER & INFO. L. 397, 401 (2004).

[8] James, *supra* note 5.

[9] 18 U.S.C. § 1037 (2010).

[10] F.T.C., FTC FACTS FOR BUSINESS, The CAN-SPAM Act: A Compliance Guide for Business (Sept. 2009), *available at* http://business.ftc.gov/sites/default/files/pdf/bus61-can-spam-act-compliance-guide-business.pdf.

[11] For example, in November 2010, a Malaysian computer expert hacked into the Federal Reserve System's computer network, and stole more than 400,000 credit card numbers. John Marzulli, *Malaysian Hacker Lin Mun Poo Nabbed in Brooklyn After Cracking into Fed Reserve Network*, N.Y. DAILY NEWS, Nov. 19, 2010, *available at* http://www.nydailynews.com/news/ny_crime/2010/11/19/2010-11-19_hacker_nabbed_after_cracking_into_fed_reserve_network.html. He was later apprehended, and eventually pled guilty to four criminal counts and could face as many as 10 years in prison. Tim Wilson, *Man Pleads Guilty To Hacking Servers At Federal Reserve Bank*, Security Dark Reading, April 18, 2011, http://www.darkreading.com/security/news/229401793/man-pleads-guilty-to-hacking-servers-at-federal-reserve-bank.html. This was just the tip of the iceberg, as cybercriminals stole or attempted to steal approximately $100 million from bank accounts in the first three quarters of 2009. Robert Lemos, *Taking Cybersecurity Lessons To The Bank*, DARK READING, Nov. 9, 2010, *available at* http://www.darkreading.com/vulnerability-management/167901026/security/news/228200593/taking-cybersecurity-lessons-to-the-bank.html.

[12] "'Malware' (malicious software) is defined as programs that are designed to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs so that users are induced into activating them." U.S. GOV'T ACCOUNTABILITY OFFICE, STATEMENT FOR THE RECORD TO THE SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY, SEN., CYBERSECURITY: CONTINUED EFFORTS ARE NEEDED TO PROTECT INFORMATION SYSTEMS FROM EVOLVING THREATS 3 n. 3 (2009), *available at* http://www.defense.gov/home/features/2010/0410_cybersec/docs/d10230t.pdf [hereinafter GAO I].

[13] Press Release, ArcSight, ArcSight and Ponemon Institute Release First Annual Cost of Cyber Crime Study (July 26, 2010), *available at* http://www.arcsight.com/press/release/arcsight-and-ponemon-institute-release-first-annual-cost-of-cyber-crime-stu/.

[14] In 2009, the Director of National Intelligence, testifying before the Senate Select Committee on Intelligence, explained that foreign nations and cybercriminals were targeting both the government and private sector in an effort to gain competitive advantages, or to disrupt or destroy them. GAO I, *supra* note

signaled a desire to use cyber attacks against the United States government.[15] And for state governments, the concern is even greater. [16] While the weak American economy has caused most states to severely trim their budgets, reducing their ability to devote expenditures to cyberdefense,[17] they remain an appealing target for cybercriminals, as their networks hold some of their citizens' most vital information, including health and driving records, educational[18] and criminal records, professional licenses, and tax information.[19] Now more than ever, proactive measures are needed to counter this evolving threat.

¶ 5 By way of summary, Part I begins with a profile of the cybercriminal, discussing the most common variety that the federal and state governments, along with American

---

12, at 1 (citing *Annual Threat Assessment of the Intelligence Community: Hearing Before the Sen. Select Comm. on Intelligence* (2009) (statement of the Director of National Intelligence)).

[15] Reports indicate that terrorists and extremists in the Middle East and South Asia may be increasingly collaborating with cybercriminals for the international movement of money, and for the smuggling of arms and illegal drugs. These links with hackers and cybercriminals may be examples of the terrorists' desire to continue to refine their computer skills, and the relationships forged through collaborative drug trafficking efforts may also provide terrorists with access to highly skilled computer programmers.

JOHN ROLLINS & CLAY WILSON, CONG. RESEARCH SERV., TERRORIST CAPABILITIES FOR CYBERATTACK: OVERVIEW AND POLICY ISSUES 2 (2007), *available at* http://www.fas.org/sgp/crs/terror/RL33123.pdf.

[16] Even small towns are subject to cyber attacks, as in September 2010, when hackers stole $600,000 from Brigantine, New Jersey after stealing the city's private online banking information. Brian Krebs, *Hackers Steal $600,000 from Brigantine, NJ*, KREBSONSECURITY, Oct. 4, 2010, http://krebsonsecurity.com/2010/10/hackers-steal-600000-from-brigantine-nj/. This came just a few months after another New Jersey town, Egg Harbor Township, lost $100,000 in a similar incident. *Id.*

[17] *See* Deloitte & NASCIO, State Governments at Risk: A call to Secure Citizen Data and Inspire Public Trust (2010), http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy2010.PDF.

[18] State university's are an especially vulnerable target, as shown in May 2009 when officials at the University of California-Berkeley announced that hackers had stolen the Social Security numbers of approximately 97,000 students, alumni, and others over the course of six months. James, *supra* note 5. Meanwhile, in September 2010, cybercriminals stole nearly $1 million from The University of Virginia's College at Wise. Brian Krebs, *Cyber Thieves Steal Nearly $1,000,000 from University of Virginia College*, KREBSONSECURITY, Sept. 1, 2010, http://krebsonsecurity.com/2010/09/cyber-thieves-steal-nearly-1000000-from-university-of-virginia-college/. The cyber thieves compromised a computer belonging to the university's comptroller, and used a computer virus to gain access to the University's bank account. *Id.* Luckily, the school was able to recover the money. *Id.*

[19] Deloitte.com, *Transcript: The Cyber Savvy State Government*, http://www.deloitte.com/view/en_US/us/Insights/Browse-by-Content-Type/podcasts/4233ed6b7e109210VgnVCM200000bb42f00aRCRD.htm. The overwhelming task facing state governments was best described by the head of Deloitte and Touche LLP's state cyber security initiative, Srini Subramanian:

> William Sutton, the notorious bank robber of the past century, once said, "I robbed banks because that is where the money is." Similarly, cyber criminals are looking at the state governments as a rich source of citizen data, also because states are perceived to have a weaker security posture compared to more regulated and better equipped organizations such as banks and financial institutions. And thus, the states face the most daunting job of protecting their growing information assets while delivering services and maintaining citizen trust.

Id.

businesses, currently face. Part II offers a robust discussion on the major forms of cybercrimes effecting the government and businesses today, including economic or foreign espionage, malicious insiders, spamming, phishing, and hacking, with a particular focus on the "botnet" form of hacking. Recent examples are provided of each cyber crime, and basic solutions are offered for reducing a company's exposure.

¶ 6 Finally, Part III discusses measures (i.e., statutes, legislation, taskforces, collaborative efforts, joint government/private sector initiatives, etc.) being taken at the federal and state levels to combat cybercrime. At the federal level, the discussion begins with action that has occurred within the executive branch since 2008, with ample time spent on the Obama Administration's recent reforms. The focus then moves to the current federal cybercrime statutory scheme, and then pending legislation in Congress. At the state level, Virginia, known for its tough approach to cybercrime, is used as a model for state action. The article then provides a multi-state survey of cybercrime related legislation from across the country.

II. PROFILING THE CYBERCRIMINAL

> *[E]very day we see waves of cyber thieves trolling for sensitive information -- the disgruntled employee on the inside, the lone hacker a thousand miles away, organized crime, the industrial spy and, increasingly, foreign intelligence services.*
>
> -- President Barack Obama[20]

¶ 7 There is no static "profile" for a cybercriminal, as they take on many forms in their effort to steal, cheat, and destroy. For American consumers and businesses, more likely then not the cybercriminal they encounter will be a male from the United States.[21] By one study, it was found that seventy-six percent of cybercriminals were male, with over half residing in either California, Florida, New York, the District of Columbia, Texas, Washington, Illinois, Georgia, New Jersey, or Nevada.[22] While California had the largest share of reported perpetrators, at 14.7%, the District of Columbia had the most cybercriminals per capita.[23] Far and away, the United States had the most cybercriminals in the world, with 65.4% of those reported residing in the country.[24]

¶ 8 For businesses, besides defending against cyber agents engaging in corporate espionage, they must be particularly wary of so-called "malicious insiders,"[25] disgruntled

[20] Obama, *supra* note 3.

[21] INTERNET CRIME COMPLAINT CENTER, 2009 INTERNET CRIME REPORT 7 (2010), www.ic3.gov/media/annualreport/2009_IC3Report.pdf.

[22] *Id.*

[23] *Id.*

[24] *Id.* at 8.

[25] "Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data." GAO I, *supra* note 12, at 4.

employees who turn their technological prowess against the company.[26] And for the government, the profiles can be even more sinister. The Government Accountability Office ("GAO") outlined six major sources of cyber threats to the federal government in their 2009 report: foreign nations, criminal groups, hackers, hacktivists,[27] disgruntled insiders,[28] and terrorists.[29] In a post-9/11 world, the prospect of a rogue cyberterrorist is particularly frightening, especially when considering some of the methods that could be used to cripple the nation:

> [A] cyberterrorist might hack into computer systems and disrupt domestic banking, the stock exchanges and international financial transactions, leading to a loss of confidence in the economy. Or he might break into an air traffic control system and manipulate it, causing planes to crash or collide. A terrorist could hack into a pharmaceutical company's computers, changing the formula of some essential medication and causing thousands to die. Or a terrorist could break into a utility company's computers, changing pressure in gas lines, tinkering with valves and causing a suburb to detonate and burn.[30]

---

[26] "The First Annual Cost of Cyber Crime Study," sponsored by ArcSight, Inc. and the Ponemon Institute, found that malicious insider attacks took as many as forty-two days to resolve, with the average cost to the company approaching $18,000 per day. Press Release, ArcSight, *supra* note 13.

[27] "Hacktivism refers to politically motivated attacks on publicly accessible Web pages or email servers. These groups and individuals overload email servers and hack into Web sites to send a political message." GAO I, *supra* note 12, at 4. Hacktivists often target powerful corporations as part of their struggle against "globalism and corporate control of the Internet" and to further their rejection of "societal ideas" such as intellectual property. Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 80 (2001), *available at* http://www-bcf.usc.edu/~idjlaw/PDF/11-1/11-1%20Rustad.pdf. A recent example of hacktivism was seen in the response to the Israeli attack against a Gaza-bound Flotilla. MCAFEE LABS, MCAFEE THREATS REPORT: SECOND QUARTER 2010 19 (2010), *available at* http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2010.pdf [hereinafter MCAFEE]. Here, hackers claiming to be Turks defaced Israeli websites and Facebook accounts owned by Israelis, while Israeli hackers infiltrated the website of a Turkish Charity. *Id.*

[28] GAO I, *supra* note 12, at 4. President Obama described the seriousness of the cyberterrorism threat:

> Al Qaeda and other terrorist groups have spoken of their desire to unleash a cyber attack on our country – attacks that are harder to detect and harder to defend against. Indeed, in today's world, acts of terror could come not only from a few extremists in suicide vests but from a few key strokes on the computer – a weapon of mass disruption.

Obama, *supra* note 3.

[29] There are two different ways to define "Cyberterrorism." Under the effects-based approach, Cyberterrorism occurs when cyberattacks cause effects that are harmful enough to spark fear similar to that of a traditional act of terrorism. The intent-based approach instead looks for cyberattacks done to further a political objective, or to cause serious harm or economic trauma. ROLLINS & WILSON, *supra* note 15, at CRS-3. If terrorists were to execute a cyberattack against the United States, the economy would be their likely focus. *Id.* at CRS-4 (citing Richard Clarke, former Counter Terrorism and National Security Advisor).

[30] Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 2002 UCLA J.L. & TECH. 3, 18 (2002), *available at* http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf.

¶ 9 Additionally, cybercriminals are not always lone wolves, but at times band together to further their criminal enterprises. For example, Koobface, a malicious program that has victimized Facebook users for over two years, was created by a criminal group operating out of St. Petersburg, Russia, and has netted the gang more than $2 million over a one year span by selling Koobface's victim's information to marketers and makers of phony antivirus software.[31] Other cybercriminal associations, such as the now defunct Shadowcrew.com, more closely resemble illicit clubs or social networks, wherein users may traffic in the databases of stolen bank account numbers, share tips on vulnerable businesses to attack, or discuss effective email scams.[32]

III. MAJOR FORMS OF CYBERCRIMES EFFECTING GOVERNMENT AND BUSINESSES TODAY

> Cyberspace is constantly under assault. Cyber spies, thieves, saboteurs, and thrill seekers break into computer systems and networks, steal personal data and trade secrets, vandalize Web sites, disrupt service, sabotage data and systems, launch computer viruses and worms, conduct fraudulent transactions, cyber-stalk, and harass individuals and companies.
>
> -- Mohammad Iqbal, *Defining Cyberterrorism*[33]

A. Economic or Foreign Espionage

¶ 10 Espionage is a hot topic in the cyber realm. In August 2010, the Department of Defense issued a report[34] discussing China's[35] increased use of "'information warfare units' to develop viruses to attack enemy computer systems and networks."[36] According

---

[31] Rivia Richmond, *Attacker That Sharpened Facebook's Defenses*, N.Y. TIMES, Nov. 14, 2010, *available at* http://www.nytimes.com/2010/11/15/technology/15worm.html.

[32] James Verini, *The Great Cyberheist*, N.Y. TIMES, Nov. 10, 2010, *available at* http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html.

[33] Iqbal, *supra* note 7, at 401.

[34] OFFICE OF THE SEC'Y. OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA 7 (2010), *available at* http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf.

[35] Even Chinese academics appear to be getting on the cyber espionage bandwagon, as Chinese researchers at the Institute of Systems Engineering of Dalian University of Technology recently published a paper describing how to attack the American power grid so as to cause a cascading failure for the entire United States. John Markoff & David Barboza, *Academic Paper in China Sets Off Alarms in U.S.*, N.Y. TIMES, Mar. 20, 2010, *available at* http://www.nytimes.com/2010/03/21/world/asia/21grid.html. The researchers claim that they were simply trying to find methods for enhancing the stability of power grids by exploring potential attack-vulnerabilities. *Id.* An independent American scientist agreed that the paper was merely theoretical and could not be used to take down the country's power grid. *Id.*

[36] Lolita C. Baldor, *Pentagon Takes Aim at China Cyber Threat*, ASSOCIATED PRESS, Aug. 19, 2010, *available at* http://www.boston.com/news/nation/washington/articles/2010/08/19/pentagon_takes_aim_at_china_cyber_threat/?page=1.

to the Pentagon, the federal government's computer systems remain a continued target of cyber intrusions from China.[37] The effectiveness of this variety of crime was witnessed in 2009, when cyber spies broke into the plans for the Pentagon's $300 billion Joint Strike Fighter project, the Defense Department's costliest weapons program ever.[38] To face this growing threat, and go on the offensive, the Pentagon has recruited "hacker soldiers" to "develop weapons that defend against, or initiate, computer attacks,"[39] and has also opened its U.S. Cyber Command, which, in 2010, took control of the various cybersecurity and cyberoffensive units that had been scattered among the military's branches.[40] The new commander of the military's cyberwarfare operations is also advocating for the creation of a "separate, secure computer network to protect civilian government agencies and critical industries like the nation's power grid against attacks mounted over the Internet."[41] This all comes as the Pentagon's interest in cyberwarfare[42] has reached what has been described as "religious intensity" by one military expert.[43] This new found fervor for cybersecurity is encouraging, but comes too late to prevent major damage from being done, as over the last ten years "[a]dversaries have acquired thousands of files from U.S. networks and from the networks of U.S. allies and industry

[37] *Id.*

[38] Siobhan Gorman et al., *Computer Spies Breach Fighter-Jet Project*, WALL ST. J., Apr. 21, 2009, *available at* http://online.wsj.com/article/SB124027491029837401.html. Further proof of the growing threat from Chinese military hackers can be seen in the diplomatic cables that were made public by Wikileaks, as these cables discuss how the Chinese military has been launching large numbers of so-called "spear-phishing" attacks against the American government and U.S. companies. Matthew J. Schwartz, *Leaked Cables Indicate Chinese Military Hackers Attacked U.S.*, INFORMATIONWEEK, April 19, 2011, *available at* http://www.informationweek.com/news/security/attacks/229401866?cid=nl_IW_daily_2011-04-19_html.

[39] Christopher Drew & John Markoff, *Contractors Vie for Plum Work, Hacking for U.S.*, N.Y. TIMES, May 30, 2009, *available at* http://www.nytimes.com/2009/05/31/us/31cyber.html. According to military experts, Northrop Grumman, General Dynamics, and Raytheon are leading the push into "offensive cyberwarfare." *Id.*

[40] Seymour M. Hersh, *The Online Threat*, THE NEW YORKER, Nov. 1, 2010, *available at* http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh.

[41] Thom Shanker, *Cyberwar Chief Calls for Secure Computer Network*, N.Y. TIMES, Sept. 23, 2010, *available at* http://www.nytimes.com/2010/09/24/us/24cyber.html?ref=computer_security. In March 2011, Cyber Command outlined the government's plan to create a "hardened IT architecture" that utilizes cloud computing and "thin-client networking" to move both data and applications off of local desktop computers and into a centralized environment, in an effort to increase cybersecurity. Elizabeth Montalbano, Cyber Command Pursues 'Defensible' IT Architecture, INFORMATIONWEEK, March 21, 2011, *available at* http://informationweek.com/news/government/security/229400008?cid=nl_IW_daily_2011-03-22_html.

[42] This growing military interest was evident in May 2009, when West Point cadets took part in a four day "cyber" war game, where they spent four days attempting to establish and maintain an operational computer network while hackers from the National Security Agency mimicked enemy cyber spies intent on infiltration. Corey Kilgannon & Noam Cohen, *Cadets Trade the Trenches for Firewalls*, N.Y. TIMES, May 10, 2009, *available at* http://www.nytimes.com/2009/05/11/technology/11cybergames.html?fta=y. Nevertheless, as of 2009, only eighty students per year graduated from the military's cyberwar schools, causing Defense Secretary Gates to note that the military is "desperately short of people who have capabilities in this area in all the services" and must call for increased resources. *Id.* The number of students graduating from these schools will quadruple in 2010 and 2011. *Id.*

[43] Drew & Markoff, *supra* note 39 (quoting Daniel T. Kuehl, military historian at the National Defense University).

partners, including weapons blueprints, operational plans, and surveillance data."[44]

¶ 11 Espionage is a similar concern for Corporate America, where trade secrets are a valuable commodity, and hackers are using military style techniques to steal confidential information from organizations.[45] Indeed, the growing threat from China-based cyber spies is not limited to the military realm, as Chinese hackers have attacked Dow Chemical and Northrop Grumman's computer networks.[46] These attacks were described as "sophisticated and precisely targeted, 'designed to get in, cover its tracks and steal corporate secrets and get out.'"[47] One commentator has described China's all out cyber-assault on American businesses as a "'full economic attack inside the United States."[48]

¶ 12 As shown by the public and private sector's vulnerability to cyber espionage, it is difficult to protect oneself from the covert activity of cyber spies. Nevertheless, individual companies can easily implement policies to reduce their exposure. For example, Porsche SE has blocked employees from using Facebook to help reduce potential access points for cyber spies,[49] as fears grow about the security threats created by social networking sites.[50] Also, some companies have gone as far as hiring former hackers to test the effectiveness of their network's cybersecurity systems,[51] though employing former cybercriminals as consultants is not without controversy and risk.[52]

---

[44] William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, FOREIGN AFFAIRS, Sept./Oct. 2010, *available at* http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain. The United States is not the only target of cyber spies, as in late November 2010, Iran's President Ahmadinejad acknowledged that "enemy" hackers had disrupted a small number of Iran's nuclear centrifuges. Kelly Jackson Higgins, *Cyberespionage at a Crossroads*, SECURITY DARK READING, Dec. 1, 2010, http://www.darkreading.com/insider-threat/167801100/security/attacks-breaches/228500103/cyberespionage-at-a-crossroads.html. According to a German software engineer, the malicious "Stuxnet" program was designed to disable Iranian centrifuges and steam turbines at a nuclear power plant that was scheduled to begin operation in 2011. John Markoff, *Worm Can Deal Double Blow to Nuclear Program*, N.Y. TIMES, Nov. 19, 2010, *available at* http://www.nytimes.com/2010/11/20/world/middleeast/20stuxnet.html.

[45] Ellen Messmer, *Cyber Espionage Seen as Growing Threat to Business, Government*, NETWORK WORLD, Jan. 17, 2008, http://www.networkworld.com/news/2008/011708-cyberespionage.html. Economic Espionage is discussed in 18 U.S.C. § 1831(a), which prohibits stealing, copying, or unlawfully possessing a trade secret for the benefit of a foreign entity or attempting or conspiring to do so. *See* DOYLE, *supra* note 6, at CRS-86.

[46] *Google Not Only Target of China Hackers*, CBSNEWS.COM, Jan. 24, 2010, http://www.cbsnews.com/stories/2010/01/24/eveningnews/main6137395.shtml.

[47] *Id.* (quoting George Kurtz, McAfee Labs).

[48] Hersh, *supra* note 40 (quoting James Lewis, a senior fellow at the Center for Strategic and International Studies).

[49] Andreas Cremer, *Porsche Blocks Staff Access to Facebook as Espionage Shield, WiWo Reports*, BLOOMBERG, http://www.bloomberg.com/news/2010-10-09/porsche-blocks-staff-access-to-facebook-as-espionage-shield-wiwo-reports.html.

[50] *See* Emily Steel & Geoffrey A. Fowler, *Facebook in Privacy Breach*, WALL ST. J., *available at* http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html; GEORGIA TECH INFO. SEC. CTR., EMERGING CYBER THREATS REPORT 2011 7 (2011), *available at* http://www.gatech.edu/inc/hgFile.php?fname=gtiscemergingthreats2011-2-1.pdf [hereinafter GEORGIA TECH].

[51] Rustad, *supra* note 27, at 82.

[52] Robert Lemos, *Commit a Crime, No Network Time?*, CNET NEWS, Apr. 16, 2003, http://news.cnet.com/Commit-a-crime,-no-network-time/2100-1009_3-997170.html. As stated by one

Later in this article, we will address the various projects that the federal government is undertaking, in concert with private industry, in an attempt to reduce the country's exposure to cyber espionage.

B. Malicious Insiders

> *One of the greatest threats to the security of client computers is not the hacker, but the enemy within: trusted company employees, ex-employees, consultants, or other insiders familiar with the computer network.*
>
> --Dr. Michael Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*[53]

¶ 13 In both the government and business context, disgruntled employees can be an especially harmful brand of cybercriminal.[54] Cybercrime studies reveal that the negative financial impact caused by insider intrusions is increasing.[55] Indeed, it has been found that "[a]lthough insider attacks may not occur as frequently as external attacks, they have a higher rate of success, can go undetected and pose a much greater risk than external attacks."[56] This insider risk became glaringly apparent in 2010, when disaffected Army Private Bradley Manning released a huge cache of classified government documents to Wikileaks, causing great havoc in the Pentagon.[57]

¶ 14 When an employee leaves a company to work for a competitor, there is always the potential that he or she will attempt to steal intellectual property. For example, the Department of Justice ("DOJ") issued a press release in September 2010 announcing that a chemist had pled guilty to stealing $20 million in trade secrets from his former

---

security analyst: "How do you explain to your shareholders that you are going to hire someone (to guard your networks) who has been jailed, not once, but multiple times . . . ." *Id.* (quoting Ira Winkler, chief security strategist for Hewlett-Packard).

[53] Rustad, *supra* note 27, at 76.

[54] "The insider threat is manifested when human behavior departs from compliance with established policies, regardless of whether it results from malice or a disregard for security policies." Frank L. Greitzer, et al., *Combating the Insider Cyber Threat*, IEEE SECURITY & PRIVACY 61 (2008), *available at* www.cert.org/archive/pdf/combatthreat0408.pdf.

[55] *Id.*

[56] Ramkumar Chinchani et. al., Towards A Theory Of Insider Threat Assessment 1 (2005) (unpublished manuscript), *available at* http://www.cse.buffalo.edu/~hungngo/papers/dsn05.pdf.

[57] Ellen Nakashima, *Messages from Alleged Leaker Bradley Manning Portray Him as Despondent Soldier*, THE WASHINGTON POST, June 10, 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/06/09/AR2010060906170.html. This incident has led to increased government measures aimed at safeguarding classified national security information from insider threats. Initial Assessments of Safeguarding and Counterintelligence Postures for Classified National Security Information in Automated Systems, Memorandum from Jacob J. Lew, Director of the Office of Management and Budget, Jan. 3, 2011, at 6, *available at* http://msnbcmedia.msn.com/i/msnbc/sections/news/OMB_Wiki_memo.pdf.

employer in anticipation of his departure for an overseas competitor.[58] The defendant admitted using his access to his employer's secure internal computer network to enter confidential databases containing trade secrets and to download approximately 160 secret formulas for paints and coatings.[59] Similarly, in July 2010, a Michigan couple was indicted for stealing and selling $40 million worth of General Motor's hybrid motor trade secrets to a Chinese automaker.[60] The employee allegedly downloaded a confidential GM document and saved thousands of pages of private GM information onto a hard drive.[61]

¶ 15 An insider may also decide to turn his technical prowess against his employer's information systems. In 2002, a computer systems administrator was charged with using a "logic bomb"[62] to cause more than $3 million in damage to his employer's computer network, as part of a plan to drive down the company's stock.[63] In July 2010, a disgruntled former senior database administrator received a year in prison for, following his firing, accessing his ex-employer's customer database, causing damage to the network and the database, and copying and saving the database to his home computer.[64] His actions resulted in a $100,000 loss to the company.[65]

¶ 16 Perhaps most dangerous is when an insider joins forces with outside criminals to wreak havoc. For example, during a year and a half span, an employee at Johns Hopkins Hospital allegedly stole patients' personal identifying information, and gave the data to four outsiders who used it to fuel a fraudulent credit card scheme that victimized fifty institutional and individual victims, causing $600,000 in damages.[66]

---

[58] Press Release, Department of Justice, Former Paint Manufacturing Chemist Pleads Guilty to Stealing Trade Secrets Valued up to $20 Million, (September 1, 2010), *available at* http://www.justice.gov/criminal/cybercrime/leePlea.pdf.

[59] *Id.*

[60] Cleopatra Andreadis, *Michigan Couple Charged with Selling GM Secrets to Chinese*, ABC.COM, July 23, 2010, http://abcnews.go.com/TheLaw/Business/michigan-couple-charged-corporate-espionage/story?id=11236400&page=1.

[61] *Id.*

[62] "Logic bombs are programmed threats which are dormant for some time before they are triggered. Once triggered, they perform a function not intended for the program in which they are embedded." Ali Peiravi & Mehdi Peiravi, *Internet Security - Cyber Crime Paradox*, 6 J. AM. SCI. 15, 17 (2010), *available at* http://www.americanscience.org/journals/am-sci/am0601/02_1046_Internet_Security_am0601.pdf.

[63] Press Release, Department of Justice, Disgruntled UBS PaineWebber Employee Charged with Allegedly Unleashing "Logic Bomb" on Company Computers (December 17, 2002), *available at* http://www.justice.gov/criminal/cybercrime/duronioIndict.htm. Similar behavior at the government-level was seen in 2001, when a subcontractor for the IRS, after being admonished for inappropriate action, inserted destructive code onto three government servers, so that once executed, the code would erase all the data on the servers. Press Release, Department of Justice, Lusby, Maryland Man Pleads Guilty to Sabotaging IRS Computers (July 24, 2001), *available at* http://www.justice.gov/criminal/cybercrime/carpenterPlea.htm.

[64] Camille Tuutti, *Disgruntled Employee-Turned-Hacker Gets a Year in Prison*, THE NEW NEW INTERNET, July 6, 2010, http://www.thenewnewinternet.com/2010/07/06/disgruntled-employee-turned-hacker-gets-a-year-in-prison/.

[65] *Id.*

[66] Robert Lemos, *Cybercriminals, Insiders May Work Together to Attack Businesses*, DARK READING, Nov. 15, 2010, *available at* http://www.darkreading.com/insider-threat/167801100/security/perimeter-security/228200983/cybercriminals-insiders-may-work-together-to-attack-businesses.html; Press Release,

¶ 17 With insider cybercriminals being especially dangerous and difficult to root out, employers must be proactive to protect their interests.[67] One method is to watch historical patterns, which might help catch an employee who, for example, regularly accessed sensitive corporate information.[68] Another is more basic, to effectively train employees so as to raise staff awareness about insider threats.[69] A noted security technologist has offered five techniques for dealing with the insider problem: (1) limit the number of users who have trusted access to the company's computer systems; (2) ensure that anyone at the company with network access has been subject to appropriate background checks; (3) limit the amount of access each user has to the network, only allowing them entry into files and applications necessary for their employment; (4) use "overlapping spheres of trust" so that no single person has unchecked authority or control on the network; and, (5) once an insider has breached the trust given to him or her, use the legal system to both prosecute the wrongdoer, and to provide a deterrent to other insiders who may have similar plans.[70] In the end, each company must assess its control system to determine if it is doing enough to protect itself from the wrath of a malicious insider.

C. Spamming, Phishing, and Email Extraction Programs

Spam may well be one of those IT problems that never completely goes away, like rust on a ship.

--Ed Sperling, Forbes.com[71]

¶ 18 Email spamming involves sending electronic mail to potentially thousands of people, often in an effort to sell a product or for data collection purposes. Amazingly, in the second quarter of 2010, spam accounted for eighty-eight percent of all email traffic.[72]

Department of Justice, Five Defendants Indicted in Fraudulent Credit Card Scheme Using Information Stolen from Johns Hopkins Hospital Patient Records (Sept. 30, 2010), *available at* http://www.justice.gov/usao/md/Public-Affairs/press_releases/press08/FiveIndictedinCreditCardSchemeUsingInformationStolenfromJohnsHopkinsPatientRecords.html.

[67] It should be noted that malicious insiders may not always be focused on stealing or destroying company information, as some may take to cyberspace to cover the tracks of past misdeeds. For example, former United States Senate candidate Joe Miller may have deleted over 15,000 emails from his government account following his resignation as an assistant attorney for the Fairbanks North Star Borough, which, if proven, could result in criminal charges. Jill Burke, *The Case of Joe Miller's Missing E-mails*, ALASKA DISPATCH, Dec. 2, 2010, *available at* http://alaskadispatch.com/dispatches/politics/7710-joe-millers-missing-e-mails-under-investigation.

[68] *Cyber Espionage a Serious Business Threat*, TECHCENTRAL.IE, Nov. 2, 2009, http://www.techcentral.ie/article.aspx?id=14239.

[69] Greitzer, *supra* note 54.

[70] Bruce Schneier, *Insiders*, SCHNEIER ON SECURITY, Feb. 16, 2009, http://www.schneier.com/blog/archives/2009/02/insiders.html.

[71] Ed Sperling, *We Can't Get Rid of Spam*, FORBES.COM, June 28, 2010, http://www.forbes.com/2010/06/26/internet-malware-security-technology-cio-network-spam.html.

[72] MCAFEE, *supra* note 27, at 4. According to McAfee, spam appears to be on an upward trend, rebounding from a decline seen in 2009 to recover to levels last seen in mid-2008. *Id.* Russia is one of the

According to Symantec, during September 2010, 92.1 percent of all email in the United States was spam.[73] Spam may be used to proliferate malware,[74] which has become especially bothersome for the public sector, as in August 2010, the government/public sector became "the most targeted industry for malware with 1 in 74.6 emails being blocked as malicious."[75] Additionally, these unsolicited emails are often the initial method that criminals employ to solicit prospective victims for money, or deceive victims into sharing private information.[76]

¶ 19 In a typical "phishing scheme," a spam email, which imitates a message from a legitimate author and is designed to steal personal information through malicious software or lure the recipient into sharing such information, is sent to a potential victim.[77] In the corporate context, phishers have sent emails claiming to be from shipping companies and banks, asserting that there is a problem with the company's shipment or bank account; the Better Business Bureau, claiming that a complaint has been filed against the company; and the courts, claiming that a subpoena has been served on the company.[78] Once the victim's personal data is disclosed or captured, it can then be used by the cybercriminal for a variety of illicit purposes, including fraud, identity theft, and for gaining unauthorized access to a computer network.[79] Even government data has been exposed by such attacks, as malware disguised as an e-Christmas card from the White House stole data from numerous government agencies in 2010, including the

---

major exporters of spam messages, and in Fall 2010, began a criminal crackdown on "SpamIt," a website that paid advertisers to send spam messages related to online pharmacies. Andrew E. Kramer, *E-Mail Spam Falls After Russian Crackdown*, N.Y. TIMES, Oct. 26, 2010, *available at* http://www.nytimes.com/2010/10/27/business/27spam.html. This resulted in a near immediate drop in spam messages by an estimated 50 billion emails per day, or approximately one-fifth of the nearly 200 billion spam messages sent daily. *Id.* This decrease will likely be temporary, as other spammers are sure to fill the void.

[73] MESSAGELABS, MESSAGELABS INTELLIGENCE SEPTEMBER 2010 6 (2010), *available at* http://www.messagelabs.com/mlireport/MLI_2010_09_September_FINAL_EN.PDF [hereinafter MESSAGELABS]. The most spammed industry sector for that month was the automotive sector, with a spam rate of 94.1 percent. *Id.* The spam rate for the public sector stood at 91.6 percent. *Id.*

[74] Malware is a problem that continues to grow, as McAfee, the well known manufacturer of anti-virus software, reported that the first half of 2010 "was the most active half-year ever for total malware production." GEORGIA TECH, *supra* note 50, at 3 (citing MCAFEE, *supra* note 27).

[75] *Id.* at 3. That number grew even more worrisome in September 2010, as 1 in 71.8 emails to the Government/Public Sector comprised a phishing attack. MESSAGELABS, *supra* note 73, at 8. Overall the phishing levels in the United States were 1 in every 907.1 emails. *Id.*

[76] USDOJ: Spam, http://www.justice.gov/spam.htm (last visited September 19, 2010).

[77] Alison Diana, *Phishers Target Social Media, Universities*, INFORMATIONWEEK, Oct. 12, 2010, http://www.informationweek.com/news/security/cybercrime/showArticle.jhtml?articleID=227701164&cid=nl_IW_daily_2010-10-15_html. Although phishing emails accounted for just two percent of total spam messages in the second quarter of 2010, as a percentage of the total spam volume, phishing was up approximately eighty-one percent from second quarter 2009 levels. MCAFEE, *supra* note 27, at 4.

[78] Internet Crime Complaint Center, et. al, *Fraud Advisory for Businesses: Corporate Account Takeover*, at 3, *available at* http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf.

[79] Diana, *supra* note 77. A recent phishing scheme used to trick victims into divulging personal information was one that claimed to be affiliated with World Cup organizers. MCAFEE, *supra* note 27, at 5. Here, the phishing message asked for the victim's occupation, his/her company name, email address, and cellular phone number. *Id.* While this information would appear to be harmless, "in the wrong hands it can be used to send spam, additional phish, or malware to mobile devices – as well as send targeted phishing or malicious emails to victims' inboxes." *Id.*

National Science Foundation's Office of Cyber Infrastructure.[80]

¶ 20 To feed the insatiable desire of spam marketers and phishers for fresh victims, hackers have developed "extraction programs" to illegally harvest the email addresses of innocent victims.[81] For example, in July 2010, the DOJ announced the guilty plea of a New Jersey man who participated in a spam email scheme that, for five years, targeted colleges and universities across America.[82] The conspirators used email extraction programs to illegally collect millions of student email addresses.[83] The group then used these email addresses to send targeted spam messages in an attempt to sell products and services to those students.[84] As part of this spam campaign, the men sent millions of email messages through the University of Missouri's computer system, causing damage to the network.[85] According to the U.S. Attorney's Office, "[n]early every college and university in the United States was impacted by this scheme," and "[t]hese schools spent significant funds to repair the damage and to implement costly preventive measures to defend themselves against future intrusions."[86]

¶ 21 While discussion of the anti-spam software, firewalls, and email filters that are available to protect employers from spam, phishers, and email-extraction programs is beyond the scope of this article,[87] every company is best served by instructing its employees to take the following simple steps to help avoid some of the negative effects of spam:

- Be careful before providing your business email address to others, especially when giving it to an online source rather than someone you have met in person, always

[80] Mathew J. Schwartz, *Spam Attack Captures Government Data*, INFORMATIONWEEK, Jan. 5, 2011, *available at* http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=229000118&cid=nl_IW_govt_2011-01-06_html.

[81] Press Release, Department of Justice, New Jersey Man Pleads Guilty to E-Mail Spam Conspiracy: Millions of E-Mail Addresses Illegally Harvested From Computers at Hundreds of Universities (July 13, 2010), *available at* http://www.cybercrime.gov/zuckerPlea.pdf.

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] Press Release, Federal Bureau of Investigation, Two Missouri Brothers Among Those Indicted in $4 Million Nationwide Spamming Conspiracy: Millions of E-Mail Addresses Illegally Harvested from Computers at 2,000 Schools (April 29, 2009), *available at* http://kansascity.fbi.gov/dojpressrel/pressrel09/kc042909.htm.

[87] Indeed, companies are often better served by outsourcing their cybersecurity management to professional cyber-defenders:

> "Nowadays, organizations need to be focused not only on their traditional perimeter defenses, but also look into external services for threat intelligence and continuous, real-time monitoring," said [Chris Rouland, CEO and co-founder of Endgame Systems]. "Whereas at one time managed security services were nice to have, they are now mandatory, the same way that your burglar alarm is generally better managed by someone else."

GEORGIA TECH, *supra* note 50, at 5.

report spam messages, and do not follow any links provided in spam emails;[88] and

- Never provide information about the organization's computer systems, including its structure or networks, to outsiders; and

- If you believe you may have revealed private information about the organization's systems, or have fallen victim to a computer virus, phishing attack, etc., report it to the proper people within the company, including network administrators. [89]

¶ 22 What these simple tips show is that creating a safe cyber-working environment for any company is about more than just software and hardware, but rather creating what one analyst has described as a "security culture."[90] For businesses, such as law firms, that deal with confidential, potentially valuable information on a daily basis, employees must understand basic concepts of cybersecurity, such as the fact that web based email systems are vulnerable to cybercriminals and should not be accessed on unsecured networks, that highly confidential information should be encrypted, that pop-up messages offering anti-virus software may actually be malicious programs, and that individual passwords to company systems must be robust enough to fend off potential hackers.[91] Indeed, for attorneys in particular, cybersecurity awareness is not just good business practice, but an ethical responsibility when dealing with the private information of clients.[92] As such, failure to adhere to industry standards on cybersecurity may even result in civil liability.[93]

---

[88] US-CERT, Cyber Security Tip ST04-007, http://www.us-cert.gov/cas/tips/ST04-007.html (last visited Sept. 19, 2010).

[89] US-CERT, Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html (last visited Sept. 19, 2010).

[90] Ed Finkel, *Cyber Space Under Siege*, A.B.A. J., Nov. 2010, at 38, 43.

[91] *Id.*; Internet Crime Complaint Center, *supra* note 78. Strong passwords include a combination of letters, symbols, and numbers. Dennis Kennedy, *Happy New Tech Year*, A.B.A. J., Jan. 2011, at 31. Attorneys and small business owners may also wish to experiment with inexpensive encryption software, such as the free "TrueCrypt." *Id.* Another useful free program, "Secunia Personal Software Inspector," performs a sweep of the programs that a computer system runs, alerting the user as to whether any security patches are necessary. *Id.*

[92] Finkel, *supra* note 90, at 40 (noting that, although currently, "breaches of client information that occur in cyberspace are subject to the same standards for lawyers that already apply outside of cyberspace," change is brewing, as Massachusetts recently enacted strong rules regarding how businesses handle the personal information of clients). Cybersecurity's ethical component originates from the fact that when a business fails to properly protect its computer systems, the resulting damage has a societal cost felt beyond the company:

> Computer users who fail to adopt efficient security measures are like businesses and consumers who do not adopt basic waste disposal practices. Both fail to implement reasonable precautions against foreseeable harm and thereby contribute to harms that impose costs on others. In other words, inadequate security results in what the economists call externalities – the costs incurred by the computer user do not reflect the costs incurred by victims, other computer users and law enforcement . . . .

Brenner & Clarke, *supra* note 4, at 696.

[93] Krottner v. Starbucks Corporation, 628 F.3d 1139 (9th Cir. 2010) (where plaintiffs were current or former Starbucks employees whose unencrypted personal information was stored on a laptop that was stolen from Starbucks, and the complaints alleged that, in failing to protect the plaintiffs' personal data, Starbucks acted negligently and breached an implied contract under state law, the Ninth Circuit found that plaintiffs had standing to sue). *But see* Krottner v. Starbucks Corporation, 2010 BL 295689 (9th Cir. 2010) (in an unpublished opinion filed with the published opinion on standing, the court found that the plaintiffs'

D. Hacking

¶ 23 Hacking is defined as "gaining unauthorized access to a computer system, programs or data."[94] Hackers sometimes crack into government or business networks for profit, for sport,[95] or for bragging rights.[96] While off-site hacking once required expertise in computer programming,[97] hackers can now retrieve attack code from the Internet, and use it against victim websites.[98] For example, a new Firefox plug-in has "made it possible for the average Joe to hijack a WiFi user's Facebook, Twitter, or other unsecured account session while sipping a cup of Joe at the local coffee shop."[99] With attack tools becoming increasingly sophisticated and user-friendly, hacking remains a major concern for systems administrators.[100]

¶ 24 A recent example of hacking's dangerous effects can be seen in the various botnet conspiracies currently plaguing the country.[101] As background, "botnets" are "collections of software agents that run automatically" to commandeer massive numbers of computers to allow cybercriminals to conduct large-scale "malicious activity including spreading spam, stealing log-in credentials and personal information or distributing malware to others."[102] In one small example, conspirators allegedly created a coded botnet program, which could be used to hack into and control another person's computer.[103] Once transmitted, the program caused the infected computers to log onto a website and wait for commands, allowing the men to control and command the botnet.[104]

¶ 25 With the botnet subject to their every whim, the men accessed, without permission, the user database of T35.net, a website which offered personal and business web-hosting services for thousands of users.[105] The database contained confidential user

---

claims failed on substantive grounds because their allegations of potential future harm, unaccompanied by present damage, were not enough to support a negligence action, and they failed to properly set forth the elements of an implied contract under state law).

[94] Goodman & Brenner, *supra* note 30, at 12.

[95] "Retreatists who break into corporate computer networks are primarily motivated by thrill-seeking, rather than economic gain." Rustad, *supra* note 27, at 78.

[96] GAO I, *supra* note 12, at 4.

[97] "In the earlier days of the computer and prior to the internet, insider computer crimes predominated and perpetrators were generally computer specialists: programmers, computer operators, data entry personnel, systems analysts, and computer managers." Rizgar Mohammed Kadir, *The Scope and the Nature of Computer Crimes Statutes – A Critical Comparative Study*, 11 GERMAN L.J. 609, 618 (2010), *available at* http://www.germanlawjournal.com/pdfs/Vol11-No6/PDF_Vol_11_No_06_609-632_RM_kadir.pdf.

[98] *See, e.g.*, Kelly Jackson Higgins, *New Firefox Plug-In Offers WiFi Cookie-Jacking For 'Average Joe'*, SECURITY DARK READING, Oct. 25, 2010, http://www.darkreading.com/insiderthreat/security/attacks/showArticle.jhtml?articleID=227900742&cid=nl_DR_daily_2010-10-26_html.

[99] *Id.*

[100] *Id.*

[101] Press Release, Department of Justice, Another Pleads Guilty in BotNet Hacking Conspiracy, June 10, 2010, *available at* http://www.cybercrime.gov/smithPlea2.pdf.

[102] GEORGIA TECH, *supra* note 50, at 3.

[103] Press release, *supra* note 101.

[104] *Id.*

[105] *Id.*

identifications and passwords, which the defendants downloaded.[106] Soon thereafter, the men defaced the T35.net website and exposed the customers' user Ids and passwords to the public.[107] And it is not only small companies that are vulnerable to botnet attacks, as in 2010, large corporations such as Google, Adobe, and several others were victimized by a targeted botnet attack called "Aurora."[108] According to an industry insider, "'the Aurora botnet was targeted against large international businesses with the goals of network infiltration, theft of business secrets and modification of critical systems data.'"[109] Another massive botnet, called Mariposa, at one time compromised data at "half of the Fortune 1000."[110]

¶ 26 This form of botnet hacking is becoming increasingly popular, as Microsoft recently announced that in the second quarter of 2010, it repaired 6.5 million botnet-infected computers, twice the number that it had cured during the second quarter of 2009.[111] This is of particular concern in the United States, the country suffering from the most botnet infections, which Microsoft measured at approximately 2.2 million American computers during the second quarter of 2010, dwarfing the number of infections experienced in runner-up Brazil, where 550,000 computers were compromised by botnet malware.[112] The growth of botnet hacking is troublesome for both government and business, as "'[b]otnets are the launch pad for much of today's criminal activity on the Internet,'" and "'[i]n many ways, they are the perfect base of operations for computer criminals.'"[113] It is for these reasons that the Georgia Tech Information Security Center, in its *Emerging Cyber Threats Report*, stated that one of the most dangerous cyber security threats in 2011 will be the "further proliferation and sophistication of botnets . . . ."[114]

---

[106] *Id.*

[107] *Id.*

[108] GEORGIA TECH, *supra* note 50, at 3.

[109] *Id.* (quoting Gunter Ollmann, Vice President of Research at Damballa). "[A] U.S. State Department cable obtained by WikiLeaks suggested the Chinese government had ordered the Aurora attack against Google." Higgins, *supra* note 44.

[110] GEORGIA TECH, *supra* note 50, at 3-4.

[111] Thomas Claburn, *Microsoft Finds U.S. Leads in Botnets*, INFORMATIONWEEK, Oct. 14, 2010, http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=227800051&cid=nl_IW_daily_2010-10-15_html.

[112] *Id.*

[113] *Id.* (quoting Adrienne Hall, general manager of Microsoft's trustworthy computing group).

[114] GEORGIA TECH, *supra* note 50, at 2. Indeed, a recent joint effort by the Department of Justice and the FBI showed how massive these botnet conspiracies can be, as the government obtained a temporary restraining order which allowed it to disable the "Coreflood" botnet. Matthew J. Schwartz, *FBI Busts Coreflood Botnet*, INFORMATIONWEEK, *available at* http://www.informationweek.com/news/security/government/229401614?cid=nl_IW_sat_2011-04-16_html. The government also obtained search warrants which allowed it to seize five command-and-control servers, located in five different states, and twenty-nine domain names used by the botnet. *Id.* This particular botnet used key-logging software to steal victim's financial information, which would then be used to remove money from the victim's bank account through wire transfers. *Id.* It is estimated that the Coreflood botnet caused at least $100 million in damages to its victims. Martha Neil, *Law Firm Loses $78K in Massive Malware Scheme That Was Disabled by Feds*, ABA JOURNAL, April 14, 2011, *available at* http://www.abajournal.com/news/article/doj_says_massive_decade-old_botnet_helped_web_thieves_steal_millions.

¶ 27 No website or web-based business is beyond the reach of a determined hacker. This was displayed in September 2010, when Twitter was rampaged by hackers who took advantage of a programming weakness to play pranks, distribute pornography, and spread worms[115] to victim-users.[116] One of the victims of the attack was the wife of the former British Prime Minister, Gordon Brown, as a link on her Twitter page sent visitors to a hard-core pornography site.[117] Another infected user was the White House's official Twitter feed.[118] Although Twitter appears to have survived the embarrassment of the attacks relatively unscathed, a hacking event could have a devastating effect on an internet-based business, hurting the company's brand and reducing user-confidence in the safety and reliability of the website.

¶ 28 As described earlier, hackers may also be associated with certain social causes, hacking not for sport, but for what they perceive as a greater societal purpose. For example, in the days following WikiLeaks release of confidential U.S. diplomatic cables, after numerous multinational corporations disassociated themselves with WikiLeaks, "hacktivists" retaliated by attacking the websites of those corporations.[119] Victims of the attacks included MasterCard, Amazon.com, PayPal, and Visa.com.[120] The cyberattacks were apparently organized by a loosely associated hacktivist group called "Anonymous."[121] Hacktivists may also work alone, like Mitchell Frost, who was recently sentenced to thirty months in prison following a 2007 attack against conservative websites, including then-presidential candidate Rudy Giuliani's Joinrudy2008.com, and the websites of Fox Commentator Bill O'Reilly and political pundit Ann Coulter.[122] Frost used the University of Akron's computer network to control a botnet, wherefrom he launched attacks against the conservative sites.[123]

¶ 29 Perhaps most disturbing is that there is recent evidence that hacking events also occur as the result of the personal vendetta of powerful leaders. For example, according to the State Department cables released by WikiLeaks, a senior member of China's Politburo Standing Committee, the group that runs the emerging world power, may have ordered that hackers attack Google after the leader "googled" himself and found articles

---

[115] "Worms are programs that can run independently. They travel from one computer to another through network connections. Worms do not change other programs. However, they may carry viruses." Peiravi & Peiravi, *supra* note 62, at 17.

[116] Bits: Business, Innovation, Technology, Society, (Sept. 21, 2010), http://bits.blogs.nytimes.com/2010/09/21/twitter-hacked-tuesday-morning/.

[117] *Id.*

[118] Barbara Ortutay, *Twitter Hacked with Tiny Virus*, ASSOCIATED PRESS, Sept. 21, 2010, *available at* http://www.chron.com/disp/story.mpl/business/7211838.html.

[119] John F. Burns & Ravi Somaiya, *Hackers Attack Those Seen as WikiLeaks Enemies*, N.Y. TIMES, Dec. 9, 2010, *available at* http://www.nytimes.com/2010/12/09/world/09wiki.html.

[120] *Id.*

[121] *Id.*

[122] Robert McMillan, *Bill O'Reilly Hacker Gets 30 Months*, CSO, Nov. 8, 2010, *available at* http://www.csoonline.com/article/634363/bill-o-reilly-hacker-gets-30-months.

[123] *Id.* Similarly, a University of Tennessee student who had hacked into former Governor Sarah Palin's email account during the last presidential campaign was recently sentenced to a year and a day in a halfway house. Bill Poovey, *Palin E-Mail Hacker Sentenced to 1 Year, 1 Day*, ASSOCIATED PRESS, Nov. 12, 2010, *available at* http://www.msnbc.msn.com/id/40152249/ns/politics-more_politics/from/toolbar.

portraying him in a negative light.[124] Such reckless use of state cyber intelligence resources is both disturbing and indicative of the efforts of certain regimes to control the press and eliminate the free exchange of political discourse on the Internet.

IV. FEDERAL AND STATE ACTION TO COMBAT CYBERCRIME

> Missiles come with a return address. Cyber attacks, for the most part, do not. For these reasons established models of deterrence do not wholly apply to cyber[security]. We need a deterrent structure that fuses offensive, defensive, and intelligence operations to meet current and future threats.
>
> -- Deputy Secretary of Defense William J. Lynn, III[125]

¶ 30 For anyone living within the United States, a major concern is what our government is doing to protect the country from cyber attacks. According to President Obama, it is "clear that we're not as prepared as we should be . . . . In recent years, some progress has been made at the federal level. But just as we failed in the past to invest in our physical infrastructure . . . we've failed to invest in the security of our digital infrastructure."[126] This discussion is best focused by addressing both legislative and executive action at the federal level, and then assessing some of the measures taken by the states.

A. Presidential Initiatives

¶ 31 In January 2008, President Bush issued a Presidential Directive establishing the Comprehensive National Cybersecurity Initiative ("CNCI").[127] The goal of this program was simple, initiate a series of projects to safeguard the executive branch with a focus on reducing vulnerabilities, defending against intrusion attempts, and preparing for future cyber threats.[128] The CNCI directive established twelve cyber defense projects, identifying lead agencies for each.[129] These projects include Trusted Internet Connections,[130] Einstein 2,[131] Einstein 3,[132] Research and Development Efforts,[133]

---

[124] James Glanz and John Markoff, *Vast Hacking by a China Fearful of the Web*, N.Y. TIMES, Dec. 4, 2010, *available at* http://www.nytimes.com/2010/12/05/world/asia/05wikileaks-china.html?_r=1.

[125] William J. Lynn III, U.S. Deputy Secretary of Defense, Remarks at Stratcom Cyber Symposium (May 26, 2010), *available at* http://www.defense.gov/speeches/speech.aspx?speechid=1477.

[126] Obama, *supra* note 3.

[127] U.S. GOV'T ACCOUNTABILITY OFFICE, CYBERSECURITY: PROGRESS MADE BUT CHALLENGES REMAIN IN DEFINING AND COORDINATING THE COMPREHENSIVE NATIONAL INITIATIVE 1 (2010), *available at* http://www.gao.gov/new.items/d10338.pdf [hereinafter GAO II].

[128] *Id.* at 1.

[129] *Id.* at 17.

[130] Led by the Office of Management and Budget ("OMB") and the Department of Homeland Security ("DHS"), this project seeks to limit "points of access to the Internet for executive branch civilian agencies." *Id.* at 18.

[131] This project, again led by DHS, deploys "passive sensors across executive branch civilian systems" that can scan the content of Internet packets to assess whether they are infected with "malicious code." *Id.*

Connecting the Centers,[134] Cyber Counterintelligence Plan,[135] Security of Classified Networks,[136] Expand Education,[137] Leap-Ahead Technology,[138] Deterrence Strategies and Programs,[139] Global Supply Chain Risk Management,[140] and Public/Private Partnerships.[141]

¶ 32 Cybersecurity remained in the spotlight when the Obama Administration took office. In February 2009, President Obama ordered a review of cybersecurity plans and programs throughout the federal government, resulting in a May 2009 report which made recommendations for improving the nation's digital infrastructure.[142] The President announced, as part of the release of this report, a "new approach" to cybersecurity:

> From now on, our digital infrastructure – the networks and computers we depend on every day – will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against

---

[132] For the Einstein 3 project, led by DHS and the Department of Defense ("DOD"), the government is pursuing development of an "intrusion prevention system" with "real-time prevention capabilities" that will "assess and block harmful code." *Id.*

[133] As part of the government's research and development efforts, led by the Office of Science and Technology Policy ("OSTP"), they are focusing on coordinating "both classified and unclassified R&D for cybersecurity. GAO II, *supra* note 127, at 18.

[134] Led by the Office of the Director of National Intelligence ("ODNI"), the "Connecting the Centers" project focuses on connecting the government's cyber centers to improve situational awareness and stimulate "greater integration and understanding of the cyber threat." *Id.*

[135] This project, led jointly by ODNI and the DOJ, seeks to development a governmentwide cyber counterintelligence plan, with efforts focused on improving the country's network's physical and electromagnetic security. *Id.* at 19.

[136] DOD and ODNI are leading this project, which seeks to improve the security of the government's classified networks. *Id.*

[137] The "Expand Education" efforts, led by DHS and DOD, emphasizes creating a "comprehensive federal cyber education and training program." *Id.*

[138] OSTP leads the "Leap-Ahead Technology" project, which is focused on developing effective new technologies "by investing in high-risk, high-reward research and development" and by partnering with both the private sector and other countries. *Id.*

[139] The National Security Council's efforts are focused on developing strategies and programs to reduce "vulnerabilities and deter interference and attack in cyberspace." GAO II, *supra* note 127, at 19.

[140] Led by DHS and DOD, this project aims at developing a multi-faceted approach to managing "global supply chain risk." *Id.*

[141] Also known as "Project 12," led by DHS, this program seeks to define the federal government's role for "extending cyber security into critical infrastructure domains" and to find new methods for the federal government and private industry to work together. *Id.* The need for public/private partnerships was discussed by David Batz, manager of Cyber & Infrastructure Security at the Edison Electric Institute:

> When you consider how much of our critical infrastructure is owned and operated by the private sector, it becomes clear that there is a need for greater public/private partnership when it comes to mitigating risk," he said. "Moving forward, government organizations that possess classified information about potential threats will need to regularly share this actionable intelligence with the private sector in a more timely and structured manner to effectively defend our nation against attacks.

GEORGIA TECH, *supra* note 50, at 10.

[142] GAO II, *supra* note 127, at 1.

> attacks and recover quickly from any disruptions or damage.[143]

¶ 33 This "new approach" included the creation of a new White House office, the Cybersecurity Coordinator,[144] who serves on the National Security Staff as well as the National Economic Council staff.[145] President Obama also named Vivek Kundra the nation's first Chief Information Officer (CIO),[146] a newly created office responsible for overseeing federal information technology spending.[147] Among the CIO's various priorities is cybersecurity.[148] Despite these efforts, the executive branch fell victim to a successful cyber attack in July 2009, when a coordinated assault spread over several days targeted the websites of several government agencies, causing major disruptions.[149]

¶ 34 In the aftermath of this attack, in March 2010, the GAO issued a report which spotlighted progress that had been made in the nation's cybersecurity, but identified remaining challenges.[150] Specifically, the report recommended better defined roles and responsibilities among key cybersecurity players at the federal level to ensure better coordination, establishing means for gauging the effectiveness of the government's cyber defense measures, creating more transparency, and making better efforts to ensure that the government has an adequate group of skilled personnel to protect federal systems.[151] These "remaining challenges" were again evident on April 8, 2010, when for nearly eighteen minutes, a state-owned Chinese telecommunications firm diverted U.S. and other foreign Internet traffic to and from American ".gov" and ".mil" sites, including sites for the Senate, the armed forces, the Defense Department, NASA, the Department of Commerce, and others, through servers in China, while also re-routing the websites of large technology companies, including Dell, Yahoo, Microsoft and IBM.[152] Although it could not be determined what China did with the diverted data, such an incident further

---

[143] Obama, *supra* note 3.

[144] Questions have been raised as to the Obama Administration's decision to make the Cybersecurity Coordinator office an executive appointment, rather than a Senate-confirmed position, as the president's critics argue that the current arrangement "will only impede congressional oversight." Ben Bain, *Senate Republicans Argue Against White House Cyber Coordinator*, WASH. TECH., June 25, 2010, http://washingtontechnology.com/blogs/cybersecurity/2010/06/bond-hatch-cyber.aspx.

[145] Obama, *supra* note 3.

[146] "Prior to joining the Obama administration, Kundra served in Mayor Fenty's cabinet as the CTO for the District of Columbia and Governor Kaine's cabinet as Assistant Secretary of Commerce and Technology for the Commonwealth of Virginia. He has also served in leadership roles in the private sector." CIO.gov, Mr. Vivek Kundra, http://www.cio.gov/Vivek-Kundra/ (last visited Oct. 22, 2010).

[147] CIO.gov, The Role of the U.S. CIO, http://www.cio.gov/module.cfm/node/about/ (last visited Oct. 22, 2010).

[148] CIO.gov, Security & Privacy, http://www.cio.gov/module.cfm/node/priorities/psec/3 (last visited Oct. 22, 2010).

[149] GAO II, *supra* note 127, at 9.

[150] GAO II, *supra* note 127.

[151] *Id.* at 4.

[152] Elizabeth Montalbano, *China Hijacked Internet Traffic from Federal Sites*, INFORMATIONWEEK, Nov. 18, 2010 (citing 2010 Report to Congress, U.S.-China Economic and Security Review Commission, *available at* http://www.uscc.gov/annual_report/2010/annual_report_full_10.pdf), *available at* http://www.informationweek.com/news/security/cybercrime/showArticle.jhtml?articleID=228300097&itc=ref-true.

demonstrates the nation's current cyber-vulnerabilities.[153]

¶ 35 Following the March report and the April attack, in June 2010, the Cybersecurity Coordinator[154] announced the release of a draft National Strategy for Trusted Identities in Cyberspace, which he described as "a blueprint to reduce cybersecurity vulnerabilities and improve online privacy protections through the use of trusted digital identities."[155] But in October 2010, another GAO report was released which found that of the twenty-four recommendations that had been made in the May 2009 cybersecurity report, only two had been fully implemented.[156] According to officials from agencies heavily involved in cybersecurity, this lag was caused by a lack of coordination among the various federal agencies, which stems from the fact that the Cybersecurity Coordinator position sat vacate for approximately seven months after President Obama announced its creation.[157] The report ultimately found that "until roles and responsibilities are made clear and the schedule and planning shortfalls . . . are adequately addressed, there is increased risk the recommendations will not be successfully completed, which would unnecessarily place the country's cyber infrastructure at risk."[158]

---

[153] *Id.*

[154] Howard Schmidt currently serves as the nation's Cybersecurity Coordinator, bringing with him forty years of experience in government, business, and law enforcement. Posting of Macon Phillips to The White House Blog, http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator (Dec. 22, 2009, 07:30 EST).

[155] Posting of Howard A. Schmidt to The White House Blog, http://www.whitehouse.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace (June 25, 2010, 14:00 EST). The Cybersecurity Coordinator went into further depth about the proposed online-identity card:

> [N]o longer should individuals have to remember an ever-expanding and potentially insecure list of usernames and passwords to login into various online services. Through the strategy we seek to enable a future where individuals can voluntarily choose to obtain a secure, interoperable, and privacy-enhancing credential (e.g., a smart identity card, a digital certificate on their cell phone, etc) from a variety of service providers – both public and private – to authenticate themselves online for different types of transactions (e.g., online banking, accessing electronic health records, sending email, etc.). Another key concept in the strategy is that the Identity Ecosystem is user-centric – that means you, as a user, will be able to have more control of the private information you use to authenticate yourself on-line, and generally will not have to reveal more than is necessary to do so.

Id. *See* U.S. DEP'T OF HOMELAND SEC., NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE (2010), *available at* http://www.dhs.gov/xlibrary/assets/ns_tic.pdf.

[156] U.S. GOV'T ACCOUNTABILITY OFFICE, CYBERSECURITY POLICY: EXECUTIVE BRANCH IS MAKING PROGRESS IMPLEMENTING 2009 POLICY REVIEW RECOMMENDATIONS, BUT SUSTAINED LEADERSHIP IS NEEDED 3 (2010), *available at* http://www.gao.gov/new.items/d1124.pdf [hereinafter GAO III].

[157] *Id.* at 4. Indeed, some would argue that the vacancy had little effect, as they perceive the Cybersecurity Coordinator position as powerless: "Schmidt has done little to assert his authority. He has no independent budget control and in a crisis would be at the mercy of those with more assets . . . ." Hersh, *supra* note 40.

[158] GAO III, *supra* note 156, at Highlights. Nevertheless, there are some heartening signs of increased cooperation between the various federal agencies. For example, in October 2010, The Department of Homeland Security and Department of Defense announced a pact that seeks to improve collaboration between the agencies and, in particular, boost the Department of Defense's data encryption and decryption capabilities. J. Nicholas Hoover, *Homeland Security, Defense Sign Cybersecurity Pact*, INFORMATIONWEEK, Oct. 14, 2010, *available at* http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=227800034.

¶ 36 Although, over the course of the last several years, the executive branch has employed proactive measures to harden the nation's cyberdefenses, the October 2010 GAO report makes clear that there is still much work left to be done. Increases in federal cybersecurity spending are a first step, as such spending is expected to increase to $13.3 billion by 2015, representing an annual enhancement of 9.1% over the next five years,[159] but spending alone will not protect our economy or confidential government information from cyber intrusions. Presidential appointments are also significant, such as President Obama's pending creation of an "internet czar" to help protect consumer privacy,[160] but such measures can only go so far. Rather, after years of federal agencies complaining about a lack of "coordination" in the nation's cybersecurity, they must now work with the Cybersecurity Coordinator to fully implement the policy recommendations of 2009, and ready the country's digital infrastructure for cyber warfare.

B. Federal Statutory Scheme

1. Federal Criminal Statutes Related to Cybercrime

¶ 37 Since various cybercrimes could be prosecuted "under at least forty different federal statutes,"[161] the following discussion provides a brief survey of just some of the severe penalties that a cybercriminal could face under federal law.

a. The CFAA[162]

¶ 38 The CFAA is a computer security statute aimed at protecting the computers operated by the federal government and banking institutions, and computers linked to the Internet.[163] It creates criminal liability for "trespassing, threats, damage, espionage," and for government computers "being corruptly used as instruments of fraud."[164] For a comprehensive discussion of § 1030, see the Congressional Research Service's report entitled *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*.[165]

---

[159] Elizabeth Montalbano, *Federal Cybersecurity Spending to Hit $13.3B by 2015*, INFORMATIONWEEK, Dec. 1, 2010, *available at* http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=228500061&cid=nl_IW_govt_2010-12-02_html.

[160] Nina Mandell, *President Obama to Announce Creation of 'Internet Czar' Position to Help Protect Consumers Privacy*, N.Y. DAILY NEWS, Nov. 12, 2010, *available at* http://www.nydailynews.com/news/politics/2010/11/12/2010-11-12_president_obama_to_announce_creation_of_internet_czar_position_to_help_protect_c.html12_president_obama_to_announce_creation_of_internet_czar_position_to_help_protect_c.html.

[161] Michael Hatcher, et al., *Computer Crimes*, 36 AM. CRIM. L. REV. 397, 410 (1999). Civil remedies are also available against cybercriminals. For example, the Anticybersquatting Consumer Protection Act, 15 U.S.C. 1125(d), "Cyberpiracy prevention," allows a civil cause of action against "cybersquatters" who register, traffic in, or use a domain name confusingly similar to or dilutive of a trademark or personal name.

[162] 18 U.S.C. § 1030.

[163] DOYLE, *supra* note 6, at 1.

[164] *Id.*

[165] *Id.*

b. Access Device Fraud[166]

¶ 39 Section 1029 outlaws the "production, use, possession, or trafficking of unauthorized or counterfeit access devices."[167] In relation to Cybercrime, the DOJ asserts that the statute could be used to prosecute a cybercriminal who employs "phishing" emails to obtain victims' private passwords and financial account numbers, or where the cybercriminal deals in stolen bank account or credit card information.[168] The penalties for this variety of fraud are severe, including civil forfeiture[169] and prison terms ranging from a maximum of ten or fifteen years for first time offenders,[170] with repeat offenders being subject to a potential twenty year jail sentence.[171]

c. Communication Interference[172]

¶ 40 The Communication Interference statute criminalizes the willful or malicious destruction of "any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States . . . ."[173] Pertinent to cybercrime, the list of covered communications systems could potentially include those used to provide email services.[174] Cybercriminals convicted under § 1362 are subject to fines and imprisonment of up to ten years.[175]

d. Stored Wire and Electronic Communications and Transactional Records Access[176]

¶ 41 This statute criminalizes the unauthorized access of email and voicemail.[177] The felony version of the crime has five basic elements: 1) intentional access;[178] 2) without or in excess of authorization;[179] 3) defendant accessed a facility where an electronic communication service (ECS) was provided;[180] 4) the defendant obtained, altered, or

---

[166] 18 U.S.C. § 1029.

[167] Cybercrime.gov, Access Device Fraud: 18 U.S.C. § 1029, http://www.justice.gov/criminal/cybercrime/ccmanual/03ccma.html#D (last visited Oct. 28, 2010).

[168] *Id.*

[169] 18 U.S.C. § 1029(c)(1)(C), (c)(2).

[170] 18 U.S.C. § 1029(c)(1)(A).

[171] 18 U.S.C. § 1029(c)(1)(B).

[172] 18 U.S.C. § 1362.

[173] *Id.*

[174] 18 U.S.C. § 1362, *available at* http://www.justice.gov/criminal/cybercrime/ccmanual/03ccma.html#G.

[175] 18 U.S.C. § 1362.

[176] 18 U.S.C. § 2701.

[177] Cybercrime.gov, Other Network Crime Statutes, http://www.cybercrime.gov/ccmanual/03ccma.html (last visited Jan. 30, 2010).

[178] *Id.*

[179] *Id.*

[180] An ECS is a facility used to transmit communications to third parties, such as an email provider, *see* FTC v. Netscape Communications Corp., 196 F.R.D. 559, 560 (N.D. Cal. 2000), or the host of an electronic bulletin board. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879-80 (9th Cir. 2002); Other Network Crime Statutes, *supra* note 177.

prevented authorized access to a wire or electronic communication while it was in "electronic storage;"[181] and (5) the defendant acted "for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act . . . ."[182] For first-time offenders who lack the fifth "purpose" element, the maximum penalty is one year imprisonment and substantial fines, while repeat violators who lack the "purpose" element, or first-time offenders who commit the act with the "purpose" discussed above, face up to five years in prison and heavy fines.[183] Repeat violations that run afoul of the improper purpose element expose the offender to a prison term of up to ten years, coupled again with extensive fines.[184]

e. Wiretap Act[185]

¶ 42 The Wiretap Act is focused on protecting the privacy of communications.[186] The Act was amended to include within its ambit electronic communications, allowing for the prosecution of computer intrusions that involve "real-time capture of information."[187] A violation under this statute includes five elements: "1) [i]ntentional; 2) interception (or endeavoring or procuring another to intercept); 3) of the contents; 4) of a wire, oral, or electronic communication; 5) by use of a device."[188] A violation of this act is a felony, with a maximum imprisonment of not more than five years and a fine.[189]

---

[181] The statutory definition of "electronic storage" is narrow, referring to the intermediate stage, incidental to the transmission, when the message is temporarily stored. 18 U.S.C. §2510(17). The nuances of this definition were discussed by the DOJ:

> For example, a copy of an email or voicemail is in 'electronic storage' only if it is at an intermediate point in its transmission and has not yet been retrieved by its intended recipient (e.g. 'unopened email'). When the recipient retrieves the email or voice mail, however, the communication reaches its final destination. If the recipient chooses to retain a copy of the communication on the service provider's system, the retained copy is no longer in "electronic storage" . . . .

Other Network Crime Statutes, *supra* note 177. Instead, "when a recipient has retrieved an email message and chooses to leave it in storage with the service provider, the email is protected under a provision of 18 U.S.C. § 2702 applicable to remote computing services." *Id. But see* Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004) (holding that emails were in electronic storage regardless of whether they had been previously accessed, and finding that previously accessed email fell within the scope of the "backup" portion of the definition of "electronic storage").

[182] 18 U.S.C. § 2701(b)(1)

[183] See 18 U.S.C. §§ 2701(b)(1)(A), (b)(2)(B), 3571(b)(3)

[184] 18 U.S.C. §§ 2701(b)(1)(B), 3571(b)(3).

[185] 18 U.S.C. § 2511.

[186] Cybercrime.gov, Wiretap Act, http://www.cybercrime.gov/ccmanual/02ccma.html#A (last visited Jan. 30, 2011) (citing S. Rep. No. 90-1097 (1968), reprinted in 1968 U.S.C.C.A.N. 2112, 2153). *See also* In re Pharmatrak, Inc., 329 F.3d 9, 18 (1st Cir. 2003) ("The paramount objective of the Wiretap Act is to protect effectively the privacy of communications").

[187] *Id.* (citing Brown v. Waddell, 50 F.3d 285, 289 (4th Cir. 1995) ("The principal purpose of the 1986 amendments to Title III was to extend to 'electronic communications' the same protections against unauthorized interceptions that Title III had been providing for 'oral' and 'wire' communications via common carrier transmissions")).

[188] Wiretap Act, *supra* note 186 (quoting 18 U.S.C. 2511(1)). "Most courts . . . have held that both wire and electronic communications are 'intercepted' within the meaning of the Wiretap Act only when such communications are acquired contemporaneously with their transmission." *Id.*

[189] 18 U.S.C. § 2511(4)(a).

f. Wire Fraud[190]

¶ 43 Another criminal tool at the government's disposal is the Wire Fraud statute. A variety of communications methods fall under the wire fraud statute, including modem and internet transmissions.[191] Violations of this statute are felonies, punishable by a fine and imprisonment of up to twenty years; with the maximum term of imprisonment rising to thirty years if the violation affects a financial institution.[192]

g. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) Act[193]

¶ 44 CAN-SPAM represents the federal government's attempt to reduce the proliferation of "spam" email, which, as discussed above, floods the email inboxes of Americans on a daily basis, and often represents an attempt to sell an unwanted good or service, or the preliminary measures of a "phisher" seeking a fresh victim. While CAN-SPAM does not outlaw unsolicited email in its entirety, it does make unsolicited commercial email unlawful if it does not allow the receiver to unsubscribe from the email pool, "contains inaccurate or misleading sender information, or is sent under or through falsified means."[194] Although CAN-SPAM preempts state anti-spam laws, its savings clause allows states to prohibit falsity or deception in the spam and preserves actions that arise out of state law that are not specific to email.[195] The act is punishable by both civil and criminal penalties.[196] The criminal provisions of CAN-SPAM are meant to address the most egregious violations of the act, and prohibit sexually explicit email that fails to include a label designating it as sexually explicit.[197]

2. Other Federal Statutes Related to Cybersecurity

a. The Sarbanes Oxley Act

¶ 45 Although the Sarbanes-Oxley Act of 2002 ("SOX"),[198] crafted in the wake of the Enron collapse, would appear to have little to do with cybersecurity, several SOX provisions impact IT professionals."[199] Specifically, because of SOX's focus on the reliability of accounting/financial records and the implementation of effective control

---

[190] 18 U.S.C. § 1343

[191] Other Network Crime Statutes, *supra* note 177 (citing United States v. Pirello, 255 F.3d 728 (9th Cir. 2001) (affirming sentence of defendant who used the Internet to commit wire fraud)).

[192] *Id.* (citing 18 U.S.C. § 1343).

[193] Pub. L. No. 108-187, 117 Stat. 2699 (criminal offenses codified at 18 U.S.C. § 1037 and 15 U.S.C. § 7704(d)).

[194] Susuk Lim, Note, *Death of the Spam Wrangler: CAN-SPAM Private Plaintiffs Required to Show Actual Harm*, 6 WASH. J. OF LAW, TECH. & ARTS 155, 157 (2010) (citing 15 U.S.C. § 7704).

[195] Katherine Wong, Note, *The Future of Spam Litigation After* Omega World Travel v. Mummagraphics, 20 HARV. J. OF LAW AND TECH. 459, 460 (2007) (citing 15 U.S.C.A. § 7707(b)).

[196] *Id.*

[197] Other Network Crime Statutes, *supra* note 177.

[198] Pub. L. No. 107-204, 116 Stat. 745, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf.

[199] Mark Rasch, *Sarbanes Oxley for IT Security?*, SECURITYFOCUS, May 2, 2005, http://www.securityfocus.com/columnists/322.

systems, it is important that companies employ an IT control system that is capable of detecting internal fraud.[200] While such insider fraud is "difficult to detect because . . . insiders frequently have intimate knowledge of the controls themselves, processes that provide for things like access control, detection of unusual account or access activity, [and] checks and balances for records relating to financial reporting may provide early warning for such fraudulent activity."[201] Additionally, although SOX is targeted at publicly traded companies, privately held companies would be well served by adopting its reform measures, including putting in place more stringent internal control systems.[202]

b. The Health Insurance Portability & Accountability Act

¶ 46 Health care providers are attractive targets for identity thieves and other cybercriminals because their records include the private health information of their patients, along with other confidential personal and financial data.[203] This was evident recently, in October 2010, when the personal information of approximately 280,000 Medicaid members, including members' health plan identification numbers and some health records, was put at risk when two insurance providers announced the loss of a storage device that contained said information.[204] Accordingly, medical entities must be vigilant in protecting their patient's sensitive digital information. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[205] helps ensure that sensitive medical, personal, and financial information is protected, as health care entities are required to implement certain cybersecurity measures in response to the HIPAA Security Rule, which "establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity" and "requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."[206]

c. The Fair and Accurate Credit Transaction Act of 2003

¶ 47 The Fair and Accurate Credit Transaction Act of 2003 ("FACTA"),[207] which

---

[200] *Id.*

[201] *Id.*

[202] *See* John Dalton & Bandana K. Kohli, *The Impact of Sarbanes-Oxley on Private Companies: An Interview with Philip Peters of Thelen Reid & Priest LLP*, 7 U.C. DAVIS BUS. L.J. 11 (2006).

[203] Cynthia M. Stamer, *Cybercrime and Identity Theft: Health Information Security Beyond HIPAA*, ABA HEALTH ESOURCE, May 2005, http://www.abanet.org/health/esource/Volume1/vol1no9/stamer.html.

[204] Tim Wilson, *Personal Data of 280,000 at Risk Following Healthcare Breach*, SECURITY DARK READING, Oct. 25, 2010, http://www.darkreading.com/database_security/security/privacy/showArticle.jhtml?articleID=227900740&cid=nl_DR_daily_2010-10-26_html.

[205] Pub. L. No. 104-191, 110 Stat. 1936, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.

[206] HHS.gov, Health Information Privacy, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/ (last visited Oct. 28, 2010). The HIPAA Security Rule is found at 45 CFR Part 160 and Subparts A and C of Part 164.

[207] Pub. L. No. 108-159, 117 Stat. 1952 (codified at 15 U.S.C. §§ 1681-1681x), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108.pdf.

amended the Fair Credit Reporting Act,[208] was adopted with the stated purpose of, among other things, preventing identity theft.[209] Under the "Red Flag" rules adopted by the FTC pursuant to FACTA,[210] financial institutions and creditors must develop and put into operation written identity theft prevention programs.[211] Those programs "must provide for the identification, detection, and response to patterns, practices, or specific activities — known as 'red flags' — that could indicate identity theft."[212] The House and Senate recently passed measures to exempt lawyers, accountants, doctors, and most other health care professionals and service providers from the rigors of the Red Flag rule.[213]

d. The Gramm-Leach-Bliley Act

¶ 48 The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act ("GLBA"),[214] includes provisions dedicated to the protection of consumer financial information held by banks, securities firms, insurance companies, and other financial institutions.[215] Specifically, the "Safeguards Rule,"[216] implemented under the GLBA, "requires financial institutions to have a security plan to protect the confidentiality and integrity of personal consumer information."[217]

e. The Digital Millennium Copyright Act (DMCA)[218]

¶ 49 The DMCA's "anti-circumvention" provisions, codified at section 1201 of the Copyright Act, were passed to "stop copyright infringers from defeating anti-piracy protections added to copyrighted works and to ban the "black box" devices intended for that purpose."[219] But, the DMCA has been viewed as more of a hindrance than a help in cybersecurity circles.[220] For example, in October 2002, the White House Cyber Security Chief voiced his concern that the DMCA was being used to chill legitimate computer security research.[221]

---

[208] 15 U.S.C. § 1681 et seq.

[209] Pub. L. No. 108-159, 117 Stat. 1952.

[210] FTC Identity Theft Rules, 16 C.F.R. § 681.1-.2 (2009).

[211] Press Release, Fed. Trade Comm'n, New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft (June 2008), *available at* http://business.ftc.gov/sites/default/files/pdf/alt050-new-red-flag-requirements-financial-institutions-and-creditors-will-help-fight-identity.pdf.

[212] *Id.*

[213] Howard Anderson, *Senate Passes Red Flags Exemptions*, GOV INFO SECURITY, Dec. 1, 2010, *available at* http://www.govinfosecurity.com/articles.php?art_id=3141; Howard Anderson, *House Approves Red Flags Exemptions*, GOV INFO SECURITY, Dec. 1, 2010, *available at* http://www.bankinfosecurity.com/articles.php?art_id=3155.

[214] Pub. L. No. 106-102, 113 Stat. 1338.

[215] Fed. Trade Comm'n, Privacy Initiatives: The Gramm-Leach Bliley Act, http://www.ftc.gov/privacy/privacyinitiatives/glbact.html (last visited Oct. 28, 2010).

[216] FTC Standards for Safeguarding Customer Information, 16 C.F.R. § 314 (2002).

[217] Fed. Trade Comm'n, Privacy Initiatives: The Safeguards Rule, http://www.ftc.gov/privacy/privacyinitiatives/safeguards.html (last visited Oct. 28, 2010).

[218] Pub. L. 105-304, 112 Stat. 2860 (1998) (codified at scattered sections of 17 U.S.C.).

[219] Fred Von Lohmann, *Unintended Consequences: Twelve Years Under the DMCA* 1, ELECTRONIC FRONTIER FOUND., Feb. 2010, http://www.eff.org/files/eff-unintended-consequences-12-years.pdf.

[220] *See id.*

[221] *See id.* at 4.

f. Federal Information Security Management Act (FISMA)[222]

¶ 50 FISMA was created to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets" and to, among other things, "provide a mechanism for improved oversight of Federal agency information security programs . . . ."[223] The act applies to government organizations, as well as the contractors and vendors that work closely with them.[224] Recently, the Department of Transportation's CIO questioned the effectiveness of FISMA audits in securing government systems. The former CIO of the Departments of Air Force and Energy echoed this concern, as he opined that the flaws such audits reveal are not always viewed in the perspective of the agencies' overall cybersecurity scheme.[225]

g. The Stored Communications Act (SCA)[226]

¶ 51 The SCA regulates government access to stored account information held by network service providers (NSPs), creating a system of privacy rights for customers and subscribers. [227] Under this scheme, § 2703 creates procedural standards that law enforcement officers must adhere to when seeking compelled disclosure of stored communications from NSPs, § 2702 regulates voluntary disclosure by NSPs of customer communications and records, while § 2701 proscribes unlawful access to certain stored communications..[228]

h. Children's Online Privacy Protection Act (COPPA)[229]

¶ 52 COPPA and its associated regulations[230] were put in place to put parents in control of what information is collected by commercial websites and online service providers on their children, under age 13, while they are online.[231] Operators covered by COPPA must:

> (1) notify parents of their information practices; (2) obtain verifiable parental consent before collecting a child's

---

[222] 44 U.S.C. § 3541.

[223] *Id.*

[224] *See* Adam Ely, 10 *Steps to Ace a FISMA Audit,* INFORMATIONWEEK, Mar. 20, 2010, *available at* http://www.informationweek.com/news/government/policy/showArticle.jhtml?articleID=224000067.

[225] *See* Eric Chabrow, *DOT CIO Questions FISMA Audits' Value*, GOVINFO SECURITY, Nov. 23, 2010, *available at* http://www.govinfosecurity.com/articles.php?art_id=3125.

[226] 18 U.S.C. §§ 2701-12.

[227] The Office of Legal Education, *Searching & Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 115, http://www.justice.gov/criminal/cybercrime/ssmanual/ssmanual2009.pdf (last visited Dec. 19, 2010).

[228] *Id.* at 115.

[229] 15 U.S.C. §§ 6501-6508.

[230] 16 C.F.R. § 312.

[231] Fed. Trade Comm'n, Frequently Asked Questions about the Children's Online Privacy Protection Rule, http://www.ftc.gov/privacy/coppafaqs.shtm (last visited Dec. 19, 2010).

> personal information; (3) give parents a choice as to whether their child's information will be disclosed to third parties; (4) provide parents access to their child's information; (5) let parents prevent further use of collected information; (6) not require a child to provide more information than is reasonably necessary to participate in an activity; and (7) maintain the confidentiality, security, and integrity of the information.[232]

i. USA PATRIOT Act[233]

¶ 53 Although not thought of as a cybersecurity measure, the USA PATRIOT Act does include some tools that could assist in the detection and prosecution of cybercrime. For example, the USA PATRIOT Act expands the circumstances under which Internet service providers can notify law enforcement of suspicious information.[234] It also adds felony acts related to the CFAA to the list of predicate offenses that can be a basis for seeking authority to intercept wire, oral, and electronic communications, allows law enforcement, under certain circumstances, to intercept communications to and from a computer trespasser, and defines certain computer crimes as acts of terrorism.[235]

j. Identity Theft and Assumption Deterrence Act of 1998 (ITADA)[236]

¶ 54 In the late 1990s, when computer-based identity theft was still in its infancy, Congress passed the ITADA in an attempt to stem this growing trend. The ITADA combated identity theft, in part, through adopting more stringent criminal measures, by amending 18 U.S.C. § 1028 to make it a federal offense to knowingly transfer or use, without authority, another person's means of identification with the intent to commit unlawful activity.[237] The ITADA also provides for a centralized complaint and consumer education service for identity theft victims, and giving the responsibility for this function to the FTC.[238] Specifically, the FTC is charged with responsibility for

---

[232] Fed. Trade Comm'n, Legal Resources – Statutes Relating to Consumer Protection Mission, http://www.ftc.gov/ogc/stat3.shtm (last visited Dec. 19, 2010).

[233] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified at scattered sections).

[234] Ellen S. Podgor, *Computer Crimes and the USA PATRIOT Act*, ABA CRIMINAL JUSTICE MAGAZINE, Summer 2002, *available at* http://www.abanet.org/crimjust/cjmag/17-2/crimes.html.

[235] *Id.*

[236] Pub. L. No. 105-318, 112 Stat 3007 (1998) (codified at 18 U.S.C.A. § 1028 and other scattered sections).

[237] Prepared Statement of The Fed. Trade Comm'n, submitted to the Comm. on Banking and Fin. Servs., U.S. House of Rep. (Betsy Broder, Asst. Dir. for the Div. of Planning and Info. of the Bureau of Consumer Protection, Fed. Trade Comm'n) (discussing 18 U.S.C. § 1028(a)(7)), *available at* http://www.ftc.gov/os/2000/09/idthefttest.htm#N_5_.

[238] *Id.*

logging the receipt of complaints by identity theft victims; providing identity theft victims with informational materials; and referring complaints to law enforcement agencies and the major consumer reporting agencies.[239]

C. Pending Federal Legislation

¶ 55 In February 2010, the House of Representatives passed H.R. 4061, the Cybersecurity Enhancement Act of 2010.[240] The bill, which the Congressional Budget Office (CBO) estimated would cost $639 million from 2010 to 2014 and $320 million thereafter,[241] would have, among other things, assisted the federal government's efforts in developing skilled personnel for its cybersecurity team, organized and prioritized the various aspects of the government's cybersecurity research and development, improved the shifting of cybersecurity technologies to the marketplace, and strengthened the role of the National Institute of Standards and Technology in developing and implementing cybersecurity public awareness and education programs to promote best practices.[242]

¶ 56 The Senate's counterpart cybersecurity legislation, S.773: Cybersecurity Act of 2010, was reported on by the Senate Committee on Commerce, Science, and Transportation in March 2010, which recommended that it be considered by the full Senate.[243] The CBO estimates that the Senate bill would cost approximately $1.4 billion from 2011 to 2015.[244] But, although congressional staffers made progress putting together a cybersecurity package that could pass the Senate, and despite the fact that Senate Majority Leader Reid emphasized passing a cybersecurity bill in 2010, industry opposition and partisan bickering stymied the passage of comprehensive reform by the 111th Congress.[245] Part of the reason for the delay may be that some members of Congress had concerns relating to increased government control of the Internet, as the Senate Bill gave the president the power to initiate contingency plans to ensure that vital federal or private services do not go offline in the event of a major cyberattack.[246] Similar concerns over presidential powers were seen in the opposition to S.3480: Protecting Cyberspace as a National Asset Act of 2010, the so-called "kill switch bill,"

---

[239] *Id.*

[240] H.R. 4061, 111th Cong. (2010), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h4061rfs.txt.pdf. The bill passed by an overwhelming, 422 to 5 vote. Govtrack.us, H.R. 4061: Cybersecurity Enhancement Act of 2010, http://www.govtrack.us/congress/bill.xpd?bill=h111-4061 (last visited Sept. 22, 2010).

[241] CONG. BUDGET OFFICE, H.R. 4061 CYBERSECURITY ENHANCEMENT ACT OF 2009 (2009), *available at* http://www.govtrack.us/data/us/111/bills.cbo/h4061.pdf.

[242] Eric Chabrow, *House Passes Cybersecurity Enhancement Act*, GOV INFO SECURITY.COM, Feb. 4, 2010, http://www.govinfosecurity.com/articles.php?art_id=2166.

[243] Govtrack.us, S. 773: Cybersecurity Act of 2010, http://www.govtrack.us/congress/bill.xpd?bill=s111-773 (last visited Sept. 22, 2010). The full text of the bill is available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:s773is.txt.pdf.

[244] CONG. BUDGET OFFICE COST ESTIMATE, S. 773 CYBERSECURITY ACT OF 2010 (2010), *available at* http://www.govtrack.us/data/us/111/bills.cbo/s773.pdf.

[245] Diane Bartz, *Analysis: Cybersecurity Bill on List for Passage This Year*, REUTERS, Sept. 9, 2010, *available at* http://www.reuters.com/article/idUSTRE6885MF20100909.

[246] Adam R. Pearlman, *Federal Cybersecurity Programs*, THE FEDERALIST SOC'Y FOR L. & PUB. POL'Y STUD., *available at* http://www.fed-soc.org/publications/pubid.1935/pub_detail.asp#_ednref2.

which would have given the president broad emergency powers to protect critical digital infrastructure following a cyber attack.[247] Another reason for the failure of comprehensive cybersecurity reform in 2010 was that the White House did little to pressure Congress to move on the bill, in part because the political value of doing so would be minimal considering that cybersecurity receives little attention from the average voter, and because the administration has been focused on improving the executive branch's readiness.[248]

¶ 57 The prospects for comprehensive reform are no better in 2011, as the looming presidential election and gridlock caused by a split Congress made one technology expert opine that "the chance of having a comprehensive anything in 2011 with this Congress is slim to none."[249]

D. State Government Action

As states confront the worst economic crisis since the Great Depression, governors across the country find themselves forced to cut many vital programs and services. Against this backdrop, it's difficult to encourage new investment; however, there is one issue that is too crucial to ignore: cybersecurity.

-- *State Governments at Risk: A call to secure citizen data and inspire public trust*[250]

1. The Virginia Model

¶ 58 As mentioned earlier, state governments are also a major target of cybercriminals. Because Virginia is the home of America Online and several other internet service

[247] Follow the bill's progress at OpenCongress, http://www.opencongress.org/bill/111-s3480/show (last visited Dec. 19, 2010). The bill would also establish the Office of Cyberspace Policy and National Center for Cybersecurity and Communications, which would be charged with setting standards and coordinating cybersecurity efforts within the federal government. *Id.*

[248] Eric Chabrow, *Cybersecurity Law: What Congress Can, Cannot Pass*, GOV INFO SECURITY, Sept. 29, 2010, http://www.govinfosecurity.com/articles.php?art_id=2961&opg=1.

[249] Grant Gross, *Congress May Be Able to Tackle Tech Issues in 2011*, Jan. 11, 2011, *available at* http://www.pcworld.com/businesscenter/article/216444/congress_may_be_able_to_tackle_tech_issues_in_2011.html (quoting Dean Garfield, president and CEO of the Information Technology Industry Council). That being said, gridlock is not the sole cause of federal inaction in the current Congressional cycle, as even when fellow Democrats suggest legislative change, there is no guarantee that the White House will put the full force of its support behind it. For example, although several Democratic members of the Senate Judiciary Committee recently called for changes to the Electronic Communications Privacy Act, 18 U.S.C. 2510 (as currently written, law enforcement agencies do not need warrants to access suspects' web-based email messages, data stored in "the cloud," and mobile-phone location information, even though they do need warrants to access email or documents stored on a suspect's computer), staffers from the Obama administration would not commit to supporting any such changes. Grant Gross, *Senators: E-surveillance law needs to be updated*, IDG NEWS SERVICE, April 7, 2011, http://www.arnnet.com.au/article/382435/senators_e-surveillance_law_needs_updated/.

[250] Deloitte, *supra* note 17, at 3.

providers, it has been dubbed "the epicenter of Internet traffic," and has adopted some of the toughest cybercrime legislation in the country.[251] For the purposes of this article, we will focus on Virginia's anti-spam legislation as a model for state government action. Virginia's other cybercrime legislation, and the laws of the other forty-nine states, are listed at the end of this paper in the "multi-state survey" section.

¶ 59 The Virginia Computer Crimes Act ("VCCA")[252] takes a multifaceted approach to cybersecurity that includes, among other things, the Virginia anti-spam statute ("VAS").[253] Although the VAS was ruled "unconstitutionally overbroad on its face" in *Jaynes v. Commonwealth* ,[254] the opinion suggested that if the spam-ban was more narrowly tailored to only prohibit unsolicited commercial emails, it could pass constitutional muster.[255] The Virginia legislature acted quickly, changing the definition of spam in the VCCA to "unsolicited commercial electronic mail."[256]

¶ 60 In its current form, the VAS criminalizes the use of "a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of spam through or into the computer network of an electronic mail service provider or its subscribers."[257] A violation of this portion of the statute is a misdemeanor, but it may be upgraded to a felony if either

> (i) the volume of spam transmitted exceeded 10,000 attempted recipients in any 24-hour time period, 100,000 attempted recipients in any 30-day time period, or one million attempted recipients in any one-year time period or (ii) revenue generated from a specific transmission of spam exceeded $1,000 or the total revenue generated from all spam transmitted to any EMSP exceeded $50,000.[258]

¶ 61 The statute also makes it a misdemeanor to knowingly sell, give, or otherwise distribute or possess with the intent to sell, give, or distribute software that

> (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of the transmission information or other routing information of spam; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of the transmission information or other routing information of

[251] Emma Scanlan, *The Fight to Save America's Inbox: State Legislation and Litigation in the Wake of CAN-SPAM*, 2 SHIDLER J. L. COM. & TECH. 12 (2005), *available at* http://www.lctjournal.washington.edu/Vol2/a012Scanlan.html.

[252] VA. CODE ANN. § 18.2-152.1 to 152.16 (2010).

[253] VA. CODE ANN. § 18.2-152.3:1 (2010).

[254] Jaynes v. Commonwealth, 666 S.E.2d 303, 314 (Va. 2008), *cert. denied*, 129 S. Ct. 1670 (2009).

[255] *Id.* at 314-15.

[256] VA. CODE ANN. § 18.2-152.2 (2010); 2010 Va. Acts 489.

[257] VA. CODE ANN. § 18.2-152.3:1(A)(1) (2010).

[258] VA. CODE ANN. § 18.2-152.3:1(B) (2010).

> spam; or (iii) is marketed by that person acting alone or with another for use in facilitating or enabling the falsification of the transmission information or other routing information of spam.[259]

¶ 62 This aggressive stance against spam is heartening, since, as discussed earlier, spam is one of the key methods through which cybercriminals engage in phishing attacks or attempt to distribute malware.[260] This anti-spam legislation has been mimicked in several other states.[261]

¶ 63 As for enforcement, the Virginia Cyber Strike Force (VCSF)[262] works in cooperation with the U.S. Attorney's Office, State Police, and the FBI to fight cybercrime.[263] The VCSF investigates and prosecutes illegal spamming, the production, distribution, and possession of child pornography, the online enticement of children, and identity theft.[264] With its comprehensive statutory framework and its enforcement measures, Virginia has been vigilant in its fight against cybercrime, and continues to serve as a model for its fellow states.

2. Multi-State Survey

¶ 64 While an excellent discussion of early state-level cybercrime legislation can be found in *State Cybercrime Legislation in the United States of America: A Survey* and *The Emerging Consensus on Criminal Conduct in Cyberspace*,[265] cybercrime and its corresponding legislation has evolved dramatically in the last decade. Accordingly, the following section provides a brief survey of current state-level legislation. The focus is on statutes aimed at preventing the type of cybercrime discussed in this article, *i.e.*, those crimes that could have a negative effect on government and business, rather than delving into such areas as online child pornography, cyber-bullying,[266] cyber-stalking, child protection registry acts, or "morals" crime. Also listed are statutes that deal with identity

---

[259] VA. CODE ANN. § 18.2-152.3:1(A)(2) (2010).

[260] *See supra* section II, subsection C.

[261] *See infra*, multi-state survey.

[262] Maria Glod, *Task Force to Combat Cyber Crimes*, THE WASH. POST, Aug. 1, 2004, *available at* http://www.washingtonpost.com/wp-dyn/articles/A20147-2004Jul28.html.

[263] Office of the Attorney General: Computer Crimes Overview, http://www.oag.state.va.us/CONSUMER/SPAM/CCUOverview.pdf (last visited Oct. 22, 2010).

[264] *Id.*

[265] Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey*, 7 RICH J. L. & TECH. 28 (2001), *available at* http://www.richmond.edu/jolt/v7i3/article2.html; Goodman & Brenner, *supra* note 30.

[266] New Jersey recently enacted what has been heralded by some as the toughest anti-bullying legislation in the country in the wake of the suicide death of Rutgers University student Tyler Clementi, whose romantic encounter with another male was secretly videotaped and live-streamed through the Internet by his dormitory roommate. N.J. Public Law 2010, Chapter 122, *available at* http://www.njleg.state.nj.us/2010/Bills/AL10/122_.PDF; Matt Friedman, *Gov. Christie Signs 'Anti-Bullying Bill of Rights'*, NJ.COM, Jan. 6, 2011, *available at* http://www.nj.com/news/index.ssf/2011/01/gov_christie_signs_anti-bullyi.html; *Times Topics: Tyler Clementi*, N.Y. TIMES, Oct. 1, 2010, *available at* http://topics.nytimes.com/top/reference/timestopics/people/c/tyler_clementi/index.html.

theft, trade secrets, and providing notifications to consumers upon IT data breaches, since each go hand-in-hand with the activities of cybercriminals. Citations to the relevant statutes for each state are provided below, along with case-law, and a notation of currently pending cyber-legislation that is relevant to the topics discussed in this article. Please note that, under certain circumstances, there may be additional grounds for criminal or civil liability in each state under more "traditional" statutes, for example, theft of services, forgery, credit card fraud, tampering with public records, or criminal mischief/trespass.

¶ 65

Alabama

- *Theft of Trademarks or Trade Secrets*
  - ALA. CODE § 13A-8-10.4 (2010)
- *Alabama Computer Crime Act*
  - ALA. CODE §§ 13A-8-100 to -103 (2010)
    - The Computer Crime Act includes:
      - *Offenses Against Intellectual Property*
        - ALA. CODE § 13A-8-102 (2010)
          - *See* Seamon v. State, 1 So. 3d 1068 (Ala. Crim. App. 2007)
      - *Offenses Against Computer Equipment or Supplies*
        - ALA. CODE § 13A-8-103 (2010)
- *The Consumer Identity Protection Act*
  - ALA. CODE §§ 13A-8-190 to -201 (2010)
    - *See* Ex parte Egbuonu, 911 So. 2d 748 (Ala. Crim. App. 2004)
- Alabama does not have security breach notification law[267]
- *Pending Legislation*
  - H.B. 482 (2010 Legislative Session)
    - Amends 13A-8-192 to increase the penalty for identity theft and remove the statute of limitations.[268]

Alaska

- *Criminal Impersonation*
  - ALASKA STAT. §§ 11.46.565 to .570 (2010)
    - *See* Phillips v. State, 211 P.3d 1148 (Alaska Ct. App. 2009)
- *Criminal Use of a Computer*
  - ALASKA STAT. § 11.46.740 (2010)
- *Deceiving a Machine*
  - ALASKA STAT. § 11.46.985 (2010)
- *Deceptive Acts or Practices Related to Spyware*

[267] State Security Breach Notification Laws, NATIONAL CONFERENCE OF STATE LEGISLATURES, Oct. 12, 2010, http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx.

[268] Bill available at http://alisondb.legislature.state.al.us/acas/ACASLoginIE.asp?SESSION=1054.

    - ALASKA STAT. §§ 45.45.792 to .798 (2010); ALASKA STAT. § 45.50.471(51) (2010)
- *Personal Information Protection Act: Disclosure of Breach of Security*
    - ALASKA STAT. § 45.48.010 (2010)
- *Limitation on Electronic Mail*
    - ALASKA STAT. § 45.50.479 (2010)
- *Pending Legislation*
    - H.B. 23
        - Would revise the "criminal use of a computer" statute to outlaw "keystroke loggers" that intercept data as it is being entered.[269]

Arizona

- *Taking/Knowingly Accepting Identity of Another Person or Entity*
    - ARIZ. REV. STAT. ANN. § 13-2008 (2010)
        - *See* State v. Sharma, 165 P.3d 693 (Ariz. Ct. App. 2007)
- *Computer Tampering*
    - ARIZ. REV. STAT. ANN. § 13-2316 (2010)
        - *See* State v. Young, 224 P.3d 944 (Ariz. Ct. App. 2010)
- *Unlawful Possession of an Access Device*
    - ARIZ. REV. STAT. ANN. § 13-2316.01 (2010)
        - *See* State v. Sharma, 165 P.3d 693 (Ariz. Ct. App. 2007)
- *Unauthorized Release of Proprietary or Confidential Computer Security Information*
    - ARIZ. REV. STAT. ANN. § 13-2316.02 (2010)
- *Interception of Electronic Communications*
    - ARIZ. REV. STAT. ANN. § 13-3005 (2010)
- *Government Access to Stored Electronic Communications*
    - ARIZ. REV. STAT. ANN. § 13-3016 (2010)
- *Commercial Electronic Mail*
    - ARIZ. REV. STAT. ANN. §§ 44-1372 to -1372.05 (2010)
- *Internet Representations*
    - ARIZ. REV. STAT. ANN. §§ 44-7201 to -7204 (2010)
- *Computer Spyware*
    - ARIZ. REV. STAT. ANN. §§ 44-7301 to -7304 (2010)
- *Notification of Breach of Security System*
    - ARIZ. REV. STAT. ANN. § 44-7501 (2010)
- *Pending Legislation*
    - None

Arkansas

- *Unsolicited Commercial and Sexually Explicit Electronic Mail Prevention Act*
    - ARK. CODE ANN. §§ 4-88-601 to -607 (2010)
- *Personal Information Protection Act*
    - ARK. CODE ANN. §§ 4-110-101 to -108 (2010)

[269] An Act Relating to Criminal Use of a Computer, H.B. No. 23, 27th Leg. 1st Sess. (Alaska 2011), *available at* http://www.legis.state.ak.us/PDF/27/Bills/HB0023A.PDF.

- *Consumer Protection Against Computer Spyware Act*
  - ARK. CODE ANN. §§ 4-111-101 to -105 (2010)
- *Identity Fraud*
  - ARK. CODE ANN. § 5-37-227 (2010)
    - *See* Whisenant v. State, 146 S.W.3d 359 (Ark. Ct. App. 2004)
- *Computer Crimes*
  - ARK. CODE ANN. §§ 5-41-101 to -109 (2010)
    - This statutory section includes:
      - *Computer Fraud*
        - ARK. CODE ANN. § 5-41-103 (2010)
          - *See* Powell v. State, 246 S.W.3d 891 (Ark. Ct. App. 2007)
      - *Computer Trespass*
        - ARK. CODE ANN. § 5-41-104 (2010)
      - *Unauthorized Computerized Communications*
        - ARK. CODE ANN. § 5-41-108 (2010)
      - *Disclosure of Personal Information by Internet Service Provider*
        - ARK. CODE ANN. § 5-41-109 (2010)
- *Computer Crimes*
  - ARK. CODE ANN. §§ 5-41-201 to -206 (2010)
    - Included within Computer Crimes are:
      - *Unlawful Acts Regarding a Computer*
        - ARK. CODE ANN. § 5-41-202 (2010)
      - *Unlawful Interference With/Use of/Access to Computers*
        - ARK. CODE ANN. § 5-41-203 (2010)
      - *Unlawful Use of Encryption*
        - ARK. CODE ANN. § 5-41-204 (2010)
      - *Unlawful Act Involving Electronic Mail*
        - ARK. CODE ANN. § 5-41-205 (2010)
      - *Computer Password Disclosure*
        - ARK. CODE ANN. § 5-41-206 (2010)
- *Arkansas Information Systems Act of 1997*
  - ARK. CODE ANN. §§ 25-4-101 to -124 (2010)
- *Pending Legislation*
  - None

California

- *Cyber Piracy*
  - CAL. BUS. & PROF. CODE §§ 17525-17528.5 (West 2010)
- *Restrictions on Unsolicited Commercial Email Advertisers*
  - CAL. BUS. & PROF. CODE §§ 17529-17529.9 (West 2010)
    - *See* Powers v. Pottery Barn, Inc., 99 Cal. Rptr. 3d 693 (Cal. Ct. App. 2009); Facebook, Inc. v. ConnectU LLC, 489 F. Supp. 2d 1087 (N.D. Cal. 2007); Asis Internet Services v. Vistaprint USA, Inc., 617 F. Supp. 2d 989 (N.D. Cal. 2009)

- *Electronic Commerce*
  - CAL. BUS. & PROF. CODE § 17538 (West 2010)
- *Consumer Protection Against Computer Spyware Act*
  - CAL. BUS. & PROF. CODE §§ 22947-22947.6 (West 2010)
- *Anti-Phishing Act of 2005*
  - CAL. BUS. & PROF. CODE §§ 22948-22948.3 (West 2010)
    - *See* Facebook, Inc. v. Jeremi Fisher, No. C 09-05842 JF (PVT), 2009 WL 5095269 (N.D. Cal. Dec. 21, 2009); Facebook, Inc. v. Wallace, No. C 09-798 JF (RS), 2009 WL 3617789 (N.D. Cal. Oct. 29, 2009); MySpace, Inc. v. Wallace, No. CV 07-1929-ABC (AGR), 2008 WL 1766714 (C.D. Cal. Apr. 15, 2008); Asis Internet Services v. Rausch, No. 08-03186 EDL, 2010 WL 1838752 (N.D. Cal. May 3, 2010)
- *Information Practices Act*
  - CAL. CIV. CODE § 1798.29 (West 2010)
- *Protection of Customer Data and Records*
  - CAL. CIV. CODE §§ 1798.80 to .84 (West 2010)
    - *See* Doe 1 v. AOL LLC, 719 F. Supp. 2d 1102 (N.D. Cal. 2010)
- *Identity Theft* (civil)
  - CAL. CIV. CODE §§ 1798.92 to .97 (West 2010)
    - *See* CTC Real Estate Serv. v. Lepe, 44 Cal. Rptr. 3d 823 (Cal. Ct. App. 2006); Satey v. JPMorgan Chase & Co., 521 F.3d 1087 (9th Cir. 2008)
- *Identity Theft* (criminal)
  - CAL. PENAL CODE §§ 530.5, 530.55 (West 2010)
    - *See* People v. Mitchell, 78 Cal. Rptr. 3d 855 (Cal. Ct. App. 2008)
- *Uniform Trade Secrets Act*
  - CAL. CIV. CODE §§ 3426 to -.11 (West 2010)
    - *See* Ajaxo Inc. v. E*Trade Fin. Corp., 115 Cal. Rptr. 3d 168 (Cal. Ct. App. 2010)
- *Trade Secrets*, *Theft/Unauthorized Copying*
  - CAL. PENAL CODE §§ 499c, 502 (West 2010)
    - *See* People v. Pribich, 27 Cal. Rptr. 2d 113 (Cal. Ct. App. 1994); People v. Laiwala, 49 Cal. Rptr. 3d 639 (Cal. Ct. App. 2006)
- *Computer Crimes*
  - CAL. PENAL CODE § 502 (West 2010)
    - *See* People v. Hawkins, 121 Cal. Rptr. 2d 627 (Cal. Ct. App. 2002); Chrisman v. City of Los Angeles, 155 Cal. App. 4th 29 (Cal. Ct. App. 2007); Facebook, Inc. v. ConnectU LLC, 489 F. Supp. 2d 1087 (N.D. Cal. 2007); People v. Hawkins, 121 Cal. Rptr. 2d 627 (Cal. Ct. App. 2002)
- *Pending Legislation*
  - None

Colorado

- *Spam Reduction Act of 2008*

- COLO. REV. STAT. § 6-1-702.5 (2010)
- *Notification of Security Breach*
  - COL. REV. STAT. § 6-1-716 (2010)
- *Theft of Trade Secrets*
  - COL. REV. STAT. § 18-4-408 (2010)
    - *See* R & D Bus. Sys. v. Xerox Corp, 152 F.R.D. 195 (D. Colo. 1993)
- *Theft of Medical Records* (definition includes computer-based records)
  - COL. REV. STAT. § 18-4-412 (2010)
- *Electronic Mail Fraud*
  - COL. REV. STAT. § 18-5-308 (2010)
- *Criminal Impersonation*
  - COL. REV. STAT. § 18-5-113 (2010)
- *Computer Crime*
  - COL. REV. STAT. § 18-5.5-101 to -102 (2010)
    - *See* People v. Rice, 198 P.3d 1241 (Colo. App. 2008)
- *Pending Legislation*
  - None

Connecticut

- *Disclosure of Security Breach of Computerized Data Containing Personal Information*
  - CONN. GEN. STAT. § 36a-701b (2010)
- *Action for Computer Related Offenses*
  - CONN. GEN. STAT. § 52-570b (2010)
    - *See* Monson v. Whitby School, Inc., No. 3:09CV1096 (MRK), 2010 WL 3023873 (D. Conn. Aug. 2, 2010)
- *Unsolicited Electronic Mail Advertising Material*
  - CONN. GEN. STAT. § 52-570c (2010)
- *Civil Action for Identity Theft*
  - CONN. GEN. STAT. § 52-571h (2010)
- *Identity Theft/Criminal Impersonation*
  - CONN. GEN. STAT. §§ 53a-129a to -130 (2010)
    - *See* State v. Schiller, 972 A.2d 272 (Conn. App. Ct. 2009)
- *Computer Crimes*
  - CONN. GEN. STAT. §§ 53-451 to -454 (2010).
    - The Computer Crimes statute includes
      - *Unauthorized Use of a Computer or Computer Network*
        - CONN. GEN. STAT. § 53-451(b) (2010)
      - *Unlawful Sale or Distribution of Software Designed to Facilitate Falsification of Electronic Mail Transmission or Routing Information*
        - CONN. GEN. STAT. § 53-451(c) (2010)
      - *Civil Actions*
        - CONN. GEN. STAT. § 53-452 (2010)
      - *Misrepresentation as On-line Internet Business*

- CONN. GEN. STAT. § 53-454 (2010)
- *Computer Crime*
  - CONN. GEN. STAT. §§ 53a-251 to -261 (2010).
    - The Computer Crime statute includes
      - *Unauthorized Access to a Computer System*
        - CONN. GEN. STAT. § 53a-251(b) (2010)
          - *See* Brantley v. City of New Haven, 920 A.2d 331 (Conn. App. Ct. 2007)
      - *Theft of Computer Services*
        - CONN. GEN. STAT. § 53a-251(c) (2010)
      - *Interruption of Computer Services*
        - CONN. GEN. STAT. § 53a-251(d) (2010)
      - *Misuse of Computer System Information*
        - CONN. GEN. STAT. § 53a-251(e) (2010)
          - *See* Monson v. Whitby School, Inc., No. 3:09CV1096 (MRK), 2010 WL 3023873 (D. Conn. Aug. 2, 2010)
      - *Destruction of Computer Equipment*
        - CONN. GEN. STAT. § 53a-251(f) (2010)
- *Computer Crime in Furtherance of Terrorist Purpose*
  - CONN. GEN. STAT. § 53a-301 (2010)
- *Pending Legislation*
  - None

Delaware

- *Computer Security Breaches*
  - DEL. CODE ANN. tit. 6, §§ 12B-101 to -104 (2010)
- *Identity Theft*
  - DEL. CODE ANN. tit. 11, § 854 (2010)
- *Computer Crime Statutes*
  - DEL. CODE ANN. tit. 11, §§ 931 to -941 (2010)
    - These Computer Crimes include:
      - *Unauthorized Access*
        - DEL. CODE ANN. tit. 11, § 932 (2010)
          - *See* State v. Boyd, No. 0707040637, 2008 WL 726900 (Del. Com. Pl. Mar. 3, 2008)
      - *Theft of Computer Services*
        - DEL. CODE ANN. tit. 11, § 933 (2010)
      - *Interruption of Computer Services*
        - DEL. CODE ANN. tit. 11, § 934 (2010)
      - *Misuse of Computer System Information*
        - DEL. CODE ANN. tit. 11, § 935 (2010)
          - *See* Wesley College v. Pitts, 974 F. Supp. 375 (D. Del. 1997)
      - *Destruction of Computer Equipment*
        - DEL. CODE ANN. tit. 11, § 936 (2010)

- *Unrequested or Unauthorized Electronic Mail or Use of Network or Software to Cause Same*
  - DEL. CODE ANN. tit. 11, § 937 (2010)
- *Failure to Promptly Cease Electronic Communication Upon Request*
  - DEL. CODE ANN. tit. 11, § 938 (2010)
- *Civil Remedies*
  - DEL. CODE ANN. tit. 11, § 941(c) (2010)
- *Pending Legislation*
  - None

Florida

- *Electronic Mail Communications Act*
  - FLA. STAT. §§ 668.60 to .610 (2010)
- *Antiphishing Act*
  - FLA. STAT. §§ 668.701 to .705 (2010)
    - *See* Pensacola Motor Sales v. E. Shore Toyota, LLC, No. 3:09cv571/RS-MD, 2010 WL 4809355 (N.D. Fla. Nov. 19, 2010); Stagl v. Gromicko, No. 3:07-cv-967-J-32TEM, 2009 WL 997193 (M.D. Fla. Apr. 14, 2009)
- *Florida Computer Crimes Act*
  - FLA. STAT. §§ 815.01 to .07 (2010)
    - Included within the Computer Crimes Act are:
      - *Offenses Against Intellectual Property*
        - FLA. STAT. § 815.04 (2010)
          - *See* Newberger v. State, 641 So. 2d 419 (Fla. Dist. Ct. App.1994); State v. Fagg, 41 So. 3d 394 (Fla. Dist. Ct. App. 2010); Garcia v. State, 939 So. 2d 1082 (Fla. Dist. Ct. App. 2006)
      - *Trade Secrets*
        - FLA. STAT. § 815.045 (2010)
          - *See* James, Hoyer, Newcomer, Smiljanich, & Yanchunis, P.A. v. Rodale, Inc., 41 So. 3d 386 (Fla. Dist. Ct. App. 2010)
      - *Offenses Against Computer Users*
        - FLA. STAT. § 815.06 (2010)
          - *See* Rodriguez v. State, 956 So. 2d 1226 (Fla. Dist. Ct. App. 2007)
- *Criminal Use of Personal Identification Information*
  - FLA. STAT. § 817.568 (2010)
    - *See* Armas v. State, 947 So. 2d 675 (Fla. Dist. Ct. App. 2007)
- *Breach of Security Concerning Confidential Personal Information in Third Party Possession*
  - FLA. STAT. § 817.5681 (2010)
- *Security of Communications*

- FLA. STAT. § 934 (2010)
  - The Security of Communications provisions include:
    - *Unlawful Access to Stored Communications*
      - FLA. STAT. § 934.21 (2010)
- *Pending Legislation*
  - None

Georgia

- *Georgia Trade Secrets Act of 1990*
  - GA. CODE ANN. §§ 10-1-760 to -767 (2010)
    - *See* Opteum Fin. Serv., LLC v. Spain, 406 F. Supp. 2d 1378 (N.D. Ga. 2005); Manuel v. Convergys Corp., 430 F.3d 1132 (11th Cir. 2005)
- *Identity Theft/Notification of Breach of Security of Personal Information*
  - GA. CODE ANN. §§ 10-1-910 to -915 (2010)
- *Georgia Computer Systems Protection Act*
  - GA. CODE ANN. §§16-9-90 to -109.1 (2010)
    - Included within Computer Systems Protection Act are:
      - *Computer Crimes (Criminal/Civil Remedies)*
        - GA. CODE ANN. §§ 16-9-90 to -94 (2010)
          - *See* Automated Drawing Sys., Inc. v. Integrated Network Serv., Inc., 447 S.E.2d 109 (Ga. Ct. App.1994); Vurv Tech. LLC v. Kenexa Corp., No. 1:08-cv-3442-WSD, 2009 WL 2171042 (N.D. Ga. July 20, 2009)
      - *Spam E-Mail*
        - GA. CODE ANN. §§ 16-9-100 to -107 (2010)
      - *Internet and Electronic Mail Fraud*
        - GA. CODE ANN. § 16-9-109.1 (2010)
- *Identity Fraud*
  - GA. CODE ANN. §§ 16-9-120 to -132 (2010)
- *Georgia Computer Security Act of 2005*
  - GA. CODE ANN. §§16-9-150 to -157 (2010)
    - Included within Computer Security Act are:
      - *Spyware, Browsers, Hijacks, and Other Software Prohibited*
        - GA. CODE ANN. §16-9-152 (2010)
      - *E-mail Virus Distribution, Denial of Service Attacks, and Other Conduct Prohibited*
        - GA. CODE ANN. §16-9-153 (2010)
      - *Inducement to Install, Copy, or Execute Software through Misrepresentation Prohibited*
        - GA. CODE ANN. § 16-9-154 (2010)
- *Pending Legislation*
  - None

Hawaii

- *Trade Secrets*
  - HAW. REV. STAT. §§ 482B-1 to -9 (2010)
    - *See* BlueEarth Biofuels, LLC v. Hawaiian Elec. Co., Inc., 235 P.3d 310 (Haw. 2010)
- *Security Breach of Personal Information*
  - HAW. REV. STAT. §§ 487N-1 to -7 (2010)
- *Identity Theft*
  - HAW. REV. STAT. §§ 708-839.6 to -.8 (2010)
    - *See* State v. Woodfall, 206 P.3d 841 (Haw. 2009)
- *Unauthorized Possession of Confidential Personal Information*
  - HAW. REV. STAT. § 708-839.55 (2010)
- *Computer Crime*
  - HAW. REV. STAT. §§ 708-890 to -895.7 (2010)
    - Computer Crime includes the following:
      - *Computer Fraud*
        - HAW. REV. STAT. §§ 708-891 to -891.5 (2010)
      - *Computer Damage*
        - HAW. REV. STAT. §§ 708-892 to -892.5 (2010)
      - *Use of a computer in the commission of a separate crime*
        - HAW. REV. STAT. § 708-893 (2010)
      - *Unauthorized Computer Access*
        - HAW. REV. STAT. §§ 708-895.5 to -895.7 (2010)
- *Pending Legislation*
  - None

Idaho

- *Computer Crime*
  - IDAHO CODE ANN. § 18-2202 (2010)
    - *See* State v. Hargrove, 67 P.3d 111 (Idaho Ct. App. 2003)
- *Misappropriation of Personal Identifying Information*
  - IDAHO CODE ANN. § 18-3126 (2010)
- *Illegal Data Processing Activities*
  - IDAHO CODE ANN. § 26-1220 (2010)
- *Identity Theft*
  - IDAHO CODE ANN. §§ 28-51-103 to -107 (2010)
    - Included within Identity Theft Act is:
      - *Disclosure of Breach of Security of Computerized Personal Information*
        - IDAHO CODE ANN. § 28-51-105 (2010)
- *Unfair Bulk Electronic Mail Advertisement Practices*
  - IDAHO CODE ANN. § 48-603E (2010)
- *Idaho Trade Secrets Act*
  - IDAHO CODE ANN. §§ 48-801 to -807 (2010)
    - *See* Basic Am., Inc. v. Shatila, 992 P.2d 175 (Idaho 1999); JustMed, Inc. v. Byce, 600 F.3d 1118 (9th Cir. 2010)

- *Pending Legislation*
  - None

Illinois

- *Computer Crime Prevention*
  - 720 ILL. COMP. STAT. 5/16D-1 to -7 (2010)
    - Included within the Computer Crime Prevention Law are:
      - *Computer Tampering*
        - 720 ILL. COMP. STAT. 5/16D-3 (2010)
          - *See* Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219 (N.D. Ill. 2005)
      - *Aggravated Computer Tampering*
        - 720 ILL. COMP. STAT. 5/16D-4 (2010)
      - *Computer Fraud*
        - 720 ILL. COMP. STAT. 5/16D-5 (2010)
          - *See* People v. Davis, 819 N.E.2d 1195 (Ill. App. Ct. 2004)
      - *Unlawful Use of Encryption*
        - 720 ILL. COMP. STAT. 5/16D-5.5 (2010)
- *Identity Theft Law (includes civil and criminal remedies)*
  - 720 ILL. COMP. STAT. 5/16G-1 to -40 (2010)
    - *See* People v. Montoya, 868 N.E.2d 389 (Ill. App. Ct. 2007)
- *Online Property Offenses*
  - 720 ILL. COMP. STAT. 5/16J-5 to -25 (2010)
    - Included in Online Property Offenses are:
      - *Online Sale of Stolen Property*
        - 720 ILL. COMP. STAT. 5/16J-10 (2010)
      - *Online Theft by Deception*
        - 720 ILL. COMP. STAT. 5/16J-15 (2010)
      - *Electronic Fencing*
        - 720 ILL. COMP. STAT. 5/16J-20 (2010)
- *Anti-Phishing Act*
  - 740 ILL. COMP. STAT. 7/1 to /15 (2010)
- *Illinois Trade Secrets Act*
  - 765 ILL. COMP. STAT. 1065/1 to /9 (2010)
    - *See* Sys. Dev. Serv., Inc. v. Haarmann, 907 N.E.2d 63 (Ill. App. Ct. 2009)
- *Electronic Mail Act*
  - 815 ILL. COMP. STAT. 511/1 to /905 (2010)
    - e360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605 (N.D. Ill. 2008)
- *Personal Information Protection Act*
  - 815 ILL. COMP. STAT. 530/1 to /30 (2010)
- *Pending Legislation*
  - H.B. 5708 (2010 Legislative Session)

- Amends the Personal Information Protection Act to include, among other things, that the "breach of the security of the system data" includes the unauthorized acquisition or use "of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a data collector."[270]

Indiana

- *Uniform Trade Secrets Act*
  - IND. CODE ANN. §§ 24-2-3-1 to -3-8 (2010)
    - *See* Patriot Homes, Inc. v. Forest River Housing, Inc., 489 F. Supp. 2d 865 (N.D. Ind. 2007); Fleming Sales Co., Inc. v. Bailey, 611 F. Supp. 507 (D.C. Ill. 1985)
- *Prohibited Spyware*
  - IND. CODE ANN. §§ 24-4.8-1 to -3 (2010)
- *Disclosure of Security Breach*
  - IND. CODE ANN. §§ 24-4.9 to 4-1-11 (2010)
    - *See* Pisciotta v. Old Nat. Bancorp, 499 F.3d 629 (7th Cir. 2007)
- *Deceptive Commercial Electronic Mail*
  - IND. CODE ANN. § 24-5-22 (2010)
- *Computer Tampering*
  - IND. CODE ANN. § 35-43-1-4 (2010)
    - *See* Sachs & Hess, P.C. v. Layer, No. 45D11-0703-PL-00026, 2009 WL 6686354 (Sup. Ct. Id. Aug. 6, 2009)
- *Computer Trespass and Computer Hoarding Programs*
  - IND. CODE ANN. § 35-43-2-3 (2010)
- *Identity Deception and Synthetic Identity Deception*
  - IND. CODE ANN. §§ 35-43-5-3.5 to -3.8 (2010)
    - *See* Prairie v. State, 914 N.E.2d 294 (Ind. Ct. App. 2009)
- *Pending Legislation*
  - None

Iowa

- *Uniform Trade Secrets Act*
  - IOWA CODE §§ 550.1 to .8 (2010)
    - *See* 205 Corp. v. Brandow, 517 N.W.2d 548 (Iowa 1994); Olson v. Nieman's, Ltd., 579 N.W.2d 299 (Iowa 1998)
- *Identity Theft-Civil Cause of Action*
  - IOWA CODE § 714.16B (2010)
- *Identity Theft-Criminal Penalties*
  - IOWA CODE § 715A.8 (2010)
    - *See* State v. Mallett, No. 02-1906, 2003 WL 22901008 (Iowa Ct. App. Dec. 10, 2003)

[270] Bill available at http://www.ilga.gov/legislation/billstatus.asp?DocNum=5708&GAID=10&GA=96&DocTypeID=HB&LegID=51040&SessionID=76.

- *Computer Spyware Protection Act*
  - IOWA CODE §§ 715.1 to .8 (2010)
- *Personal Information Security Breach Protection*
  - IOWA CODE §§ 715C.1 to .2 (2010)
- *Unauthorized Computer Access (civil and criminal relief)*
  - IOWA CODE § 716.6B (2010)
- *Electronic Mail (civil and criminal relief)*
  - IOWA CODE §§ 716A.1 to .7 (2010)
    - *See* Kramer v. Perez, 595 F.3d 825 (8th Cir. 2010)
- *Pending Legislation*
  - None

Kansas

- *Identity Theft/Fraud*
  - KAN. STAT. ANN. § 21-4018 (2010)
    - *See* State v. Hardesty, 213 P.3d 745 (Kan. Ct. App. 2009); State v. Meza, 165 P.3d 298 (Kan. Ct. App. 2007); City of Liberal v. Vargas, 24 P.3d 155 (Kan. Ct. App. 2001)
- *Uniform Trade Secrets Act*
  - KAN. STAT. ANN. §§ 60-3320 to 3330 (2010)
    - *See* Evolution, Inc. v. SunTrust Bank, 342 F. Supp. 2d 943 (D. Kan. 2004)
- *Computer Crime; Computer Password Disclosure; Computer Trespass*
  - KAN. STAT. ANN. § 21-3755 (2010)
    - *See* State v. Allen, 917 P.2d 848 (Kan. 1996); State v. Rupnick, 125 P.3d 541 (Kan. 2005)
- *Commercial Electronic Mail Act*
  - KAN. STAT. ANN. § 50-6,107 (2010)
    - *See* Fenn v. Mleads Enter., Inc., 137 P.3d 706 (Utah 2006)
- *Protection of Consumer Information*
  - KAN. STAT. ANN. §§ 50-7a01 to -7a04 (2010)
- *Pending Legislation*
  - None

Kentucky

- *Uniform Trade Secrets Act*
  - KY. REV. STAT. ANN. §§ 365.880 to .900 (2010)
    - *See* Fastenal Co. v. Crawford, 609 F. Supp. 2d 650 (E.D. Ky. 2009)
- *Phishing*
  - KY. REV. STAT. ANN. § 434.697 (2010)
- *Unlawful Access to a Computer*
  - KY. REV. STAT. ANN. §§ 434.840 to .853 (2010)
    - *See* Com. v. Cocke, 58 S.W.3d 891 (Ky. Ct. App. 2001)
- *Misuse of Computer Information*
  - KY. REV. STAT. ANN. § 434.855 (2010)

- *Theft of Identity*
  - KY. REV. STAT. ANN. § 514.160 (2010)
    - *See* Crouch v. Com., 323 S.W.3d 668 (Ky. 2010)
- Kentucky does not have a security breach law[271]
- *Pending Legislation*
  - H.B. 581 (2010 Legislative Session)
    - This bill creates new sections of KRS Chapter 367, providing definitions related to identity theft and requiring a business to give notice to a person whose personal information was compromised in a security breach.[272]

Louisiana

- *Identity Theft*
  - LA. REV. STAT. ANN. § 14:67.16 (2010)
    - *See* State v. Jacobs, 2 So. 3d 1289 (La. App. 2009)
- *Offenses Against Intellectual Property*
  - LA. REV. STAT. ANN. § 14:73.2 (2010)
    - *See* State v. Tanner, 534 So.2d 535 (La. Ct. App. 1988)
- *Offenses Against Computer Equipment or Supplies*
  - LA. REV. STAT. ANN. § 14:73.3 (2010)
- *Offenses Against Computer Users*
  - LA. REV. STAT. ANN. § 14:73.4 (2010)
- *Computer Fraud*
  - LA. REV. STAT. ANN. § 14:73.5 (2010)
    - *See* State v. Azar, 539 So. 2d 1222 (La. 1989)
- *Offenses Against Electronic Mail Service Provider*
  - LA. REV. STAT. ANN. § 14:73.6 (2010)
    - *See* Fox v. Reed, No. CIV A 99-3094, 2000 WL 288379 (E.D. La. Mar. 16, 2000)
- *Computer Tampering*
  - LA. REV. STAT. ANN. § 14:73.7 (2010)
- *Unsolicited Commercial Electronic Mail*
  - LA. REV. STAT. ANN. § 51:2003 (2010)
- *Consumer Protection against Computer Spyware*
  - LA. REV. STAT. ANN. §§ 51:2006 to :2014 (2010)
- *Louisiana Anti-Phishing Act*
  - LA. REV. STAT. ANN. §§ 51:2021 to 51:2025 (2010)
- *Anti-Phishing Act of 2006*
  - LA. REV. STAT. ANN. §§ 51:2031 to 51:2034 (2010)
- *Database Security Breach Notification Law*
  - LA. REV. STAT. ANN. §§ 51:3071 to 3077 (2010)
    - *See* Belle Chasse Auto. Care, Inc. v. Advanced Auto Parts, Inc., No. 08-1568, 2009 WL 799760 (E.D. La. Mar. 24, 2009)
- *Pending Legislation*

[271] State Security Breach Notification Laws, *supra* note 267.
[272] Bill available at http://www.lrc.state.ky.us/record/10rs/hb581.htm.

- None

Maine

- *Identity Theft*
  - ME. REV. STAT. ANN. tit. 17-A, §§ 354-2A, 905-A (2010)
    - *See* State v. Radley, 804 A.2d 1127 (Me. 2002)
- *Criminal Invasion of Computer Privacy*
  - ME. REV. STAT. ANN. tit. 17-A, §§ 431, 433 (2010)
- *Notice of Risk to Personal Data*
  - ME. REV. STAT. ANN. tit. 10, §§ 1346, 1350-B (2010)
- *Electronic Mail Solicitation Restricted*
  - ME. REV. STAT. ANN. tit. 10, § 1497 (2010)
- *Uniform Trade Secrets Act*
  - ME. REV. STAT. ANN. tit. 10, §§ 1541, 1548 (2010)
    - *See* Officemax Inc. v. County Qwick Print, Inc., No. CV-10-110-B-W, 2010 WL 4473306 (D. Me. Nov. 8, 2010); Diamond Phoenix Corp. v. Small, No. 05-79-P-H, 2005 WL 1530264 (D. Me. June 28, 2005)
- *Pending Legislation*
  - None

Maryland

- *Spam Deterrence*
  - MD. CODE ANN. CRIM. LAW § 3-805.1 (2010)
    - *See* Beyond Sys., Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523 (D. Md. 2006)
- *Unauthorized Access to Computers and Related Material*
  - MD. CODE ANN. CRIM. LAW § 7-302 (2010)
    - *See* Briggs v. State, 704 A.2d 904 (Md. 1998).
- *Identity Fraud*
  - MD. CODE ANN. CRIM. LAW §§ 8-301 to -305 (2010)
    - *See* Clark v. State, 981 A.2d 710 (Md. Ct. Spec. App. 2009); Ishola v. State, 945 A.2d 1273 (Md. 2008)
- *Maryland Uniform Trade Secrets Act*
  - MD. CODE ANN. COM. LAW §§ 11-1201 to -1209 (2010)
    - *See* Systems 4, Inc. v. Landis & Gyr, Inc., 8 F. App'x. 196 (4th Cir. 2001)
- *Commercial Electronic Mail*
  - MD. CODE ANN. COM. LAW § 14-3001 to -3003 (2010)
    - *See* Beyond Sys., Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523 (D. Md. 2006)
- *Security Breach*
  - MD. CODE ANN. COM. LAW §§ 14-3501 to 3508 (2010)
- *Pending Legislation*
  - None

Massachusetts

- *Obtaining Computer Services by Fraud or Misrepresentation*
  - MASS. GEN. LAWS ANN. ch. 266 § 33A (2010)
- *Use of Personal Identification of Another; Identity Fraud*
  - MASS. GEN. LAWS ANN. ch. 266 § 37E (2010)
    - *See* Com. v. Giavazzi, 802 N.E.2d 589 (Mass. App. Ct. 2004)
- *Stolen Trade Secrets*
  - MASS. GEN. LAWS ANN. ch. 266 § 60A (2010)
- *Unauthorized Access to Computer System*
  - MASS. GEN. LAWS ANN. ch. 266 § 120F (2010)
    - *See* Com. v. Piersall, 853 N.E.2d 210 (Mass. App. Ct. 2006)
- *Security Breaches*
  - MASS. GEN. LAWS ANN. ch. 93h §§1-6 (2010)
- *Pending Legislation*
  - H227/332 (2010 Legislative Session)
    - Legislation relating to spyware.[273]
  - H313 (2010 Legislative Session)
    - Legislation to further regulate online advertising.[274]
  - H1545/1550 (2010 Legislative Session)
    - Legislation involving computer crimes.[275]
  - H326/3427 (2010 Legislative Session)
    - Legislation relating to identity theft.[276]

Michigan

- *Identity Theft Protection Act*
  - MICH. COMP. LAWS §§ 445.61 to .77 (2010), § 445.903(jj)
    - Included within this Act is:
      - *Notice of Security Breach*
        - MICH. COMP. LAWS § 445.72 (2010)
- *Uniform Trade Secrets Act*
  - MICH. COMP. LAWS §§ 445.1901 to .1910 (2010)
    - *See* Stromback v. New Line Cinema, 384 F.3d 283 (6th Cir. 2004); Kelly Serv. v. Eidnes, 530 F. Supp. 2d 940 (E.D. Mich. 2008)
- *Unsolicited Commercial E-mail Protection Act*
  - MICH. COMP. LAWS §§ 445.2501 to .2508 (2010)
- *Fraudulent Access to Computers, Computer Systems, and Computer Networks*
  - MICH. COMP. LAWS §§ 752.791 to .797 (2010)
    - *See* Martinez v. Mueller, No. 266200, 2006 WL 1115534 (Mich. Ct. App. Apr. 27, 2006); People v. Jemison, 466 N.W.2d 378

[273] Bills available at http://www.malegislature.gov/Bills/186/House/H227 and http://www.malegislature.gov/Bills/186/House/H332.

[274] Bill available at http://www.malegislature.gov/Bills/186/House/H313.

[275] Bills available at http://www.malegislature.gov/Bills/186/House/H1545 and http://www.malegislature.gov/Bills/186/House/H1550.

[276] Bills available at http://www.malegislature.gov/Bills/186/House/H326 and http://www.malegislature.gov/Bills/186/House/H3427.

(Mich. Ct. App. 1991); People v. Golba, 729 N.W.2d 916 (Mich. Ct. App. 2007)

- *Pending Legislation*
  - S.B. 149 (2010 Legislative Session)
    - Amends the Identity Theft Protection Act to include, among other things, a prohibition against sending an email or creating a webpage that seeks to induce an individual to provide personal identifying information with the intent of using that information to commit identity theft.[277]
  - S.B. 223 (2010 Legislative Session)
    - Establishes and increases penalties for identity theft.[278]
  - S.B. 717 (2010 Legislative Session)
    - Create the information security program standards act, provides for standards for safeguarding personal information, and provides for certain civil immunity.[279]

Minnesota

- *Data Warehouses; Notice Required For Certain Disclosures*
  - MINN. STAT. ANN. § 325E.61 (2010)
- *False or Misleading Commercial Electronic Mail Messages*
  - MINN. STAT. § 325F.694 (2010)
- *Identity Theft*
  - MINN. STAT. ANN. § 609.527 (2010)
- *Crimes Against Commerce*
  - This statutory section includes:
    - *Computer Crime*
      - MINN. STAT. ANN. § 609.87 (2010)
    - *Computer Damage*
      - MINN. STAT. ANN. § 609.88 (2010)
        - *See* Am. Computer Trust Leasing v. Jack Farrell Implement Co., 763 F.Supp. 1473 (D. Minn. 1991)
    - *Computer Theft*
      - MINN. STAT. ANN. § 609.89 (2010)
        - *See American Computer Trust Leasing v. Jack Farrell Implement Co.,* 763 F. Supp. 1473 (D. Minn. 1991)
    - *Unauthorized Computer Access*
      - MINN. STAT. ANN. § 609.891 (2010)
    - *Criminal Use of Encryption*
      - MINN. STAT. ANN. § 609.8912 (2010)

---

[277] Bill available at http://www.legislature.mi.gov/documents/2009-2010/billconcurred/Senate/pdf/2009-SCB-0149.pdf.

[278] Bill available at http://www.legislature.mi.gov/documents/2009-2010/billconcurred/Senate/pdf/2009-SCB-0223.pdf.

[279] Bill available at http://www.legislature.mi.gov/documents/2009-2010/billintroduced/Senate/pdf/2009-SIB-0717.pdf.

        - *Facilitating Access to Computer Security System*
            - MINN. STAT. ANN. § 609.8913 (2010)
- *Unlawful Access to Stored Communications*
    - MINN. STAT. ANN. § 626A.26 (2010)
        - *See* Am. Computer Trust Leasing v. Jack Farrell Implement Co., 763 F. Supp. 1473 (D. Minn. 1991); Gates v. Wheeler, No. A09-2355, 2010 WL 4721331 (Minn. Ct. App. Nov. 23, 2010)
- *Disclosure of Contents*
    - MINN. STAT. ANN. § 626A.27 (2010)
        - *See* Am. Computer Trust Leasing v. Jack Farrell Implement Co., 763 F. Supp. 1473 (D. Minn. 1991)
- *Pending Legislation*
    - H3850 (2010 Legislative Session)
        - A bill enhancing the enforcement capability for identity theft and other fraudulent activities conducted electronically.[280]

Mississippi

- *Mississippi Uniform Trade Secrets Act*
    - MISS. CODE ANN. §§ 75-26-1 to -19 (2010)
        - *See* Union Nat. Life Ins. Co. v. Tillman, 143 F. Supp. 2d 638 (N.D. Miss. 2000); Pepper v. Int'l Gaming Sys., LLC, 312 F. Supp. 2d 853 (N.D. Miss. 2004); Marshall v. Gipson Steel, Inc., 806 So. 2d 266 (Miss. 2002)
- *Fraudulent Use of Identity*
    - MISS. CODE ANN. § 97-19-85 (2010)
        - *See* Serrato-Soto v. Holder, 570 F.3d 686 (6th Cir. 2009); Catling v. State, 45 So. 3d 295 (Miss. Ct. App. 2010)
- *Computer Crimes and Identity Theft*
    - MISS. CODE ANN. §§ 97-45-1 to -31 (2010)
        - This Act includes
            - *Identity Theft*
                - MISS. CODE ANN. §§ 97-45-2 to -19 (2010)
            - *Computer Fraud*
                - MISS. CODE ANN. § 97-45-3 (2010)
            - *Offense Against Computer Users*
                - MISS. CODE ANN. § 97-45-5 (2010)
            - *Offense Against Computer Equipment*
                - MISS. CODE ANN. § 97-45-7 (2010)
            - *Offense Against Intellectual Property*
                - MISS. CODE ANN. § 97-45-9 (2010)
- *Pending Legislation*
    - H.B. 583
        - Notice of breach of security requirements[281]
            - Effective July 1, 2011

[280] Bill available at http://wdoc.house.leg.state.mn.us/leg/LS86/HF3850.0.pdf.
[281] Bill available at http://billstatus.ls.state.ms.us/2010/pdf/history/HB/HB0583.xml.

Missouri

- *Unsolicited Electronic Mail Without Either Return Email Address or Toll-Free Number Prohibited*
  - MO. REV. STAT. § 407.1123 (2010)
- *Interactive Computer Service May Block Certain Electronic Mail Without Liability*
  - MO. REV. STAT. § 407.1132 (2010)
- *Notice to Consumer for Breach of Security*
  - MO. REV. STAT. § 407.1500 (2010)
    - *See* Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046 (E.D. Mo. 2009)
- *The Missouri Uniform Trade Secrets Act*
  - MO. REV. STAT. §§ 417.450 to .467 (2010)
    - *See* BP Chem. Ltd. v. Jiangsu Sopo Corp., 429 F. Supp. 2d 1179 (E.D. Mo. 2006)
- *Tampering With Computer Data, Computer Equipment, or Computer Users*
  - MO. REV. STAT. § 537.525 (2010)
    - See Chrysler Corp. v. Carey, 5 F. Supp. 2d 1023 (E.D. Mo. 1998)
- *Identity Theft*
  - MO. REV. STAT. § 570.223 (2010)
- *Pending Legislation*
  - None

Montana

- *Notification of Breach of Security of Data System*
  - MONT. CODE ANN. § 2-6-504 (2010)
- *Uniform Trade Secrets Act*
  - MONT. CODE ANN. §§ 30-14-401 to -409 (2010)
    - *See* Great Falls Tribune v. Montana Pub. Serv. Com'n, 82 P.3d 876 (Mont. 2003)
- *Impediment of Identity Theft*
  - MONT. CODE ANN. §§ 30-14-1701 to -1736 (2010))
    - This Act includes
      - *Computer Security Breach*
        - MONT. CODE ANN. § 30-14-1704 (2010)
      - *Fraudulent Electronic Misrepresentation*
        - MONT. CODE ANN. § 30-14-1712 (2010)
- *Fraudulent Electronic Misrepresentation*
  - MONT. CODE ANN. § 33-19-410 (2010)
- *Unlawful Use of a Computer*
  - MONT. CODE ANN. §§ 45-6-310 to -311 (2010)
- *Theft of Identity*
  - MONT. CODE ANN. § 45-6-332 (2010)
- *Pending Legislation*
  - None

Nebraska

- *Criminal Impersonation*
  - NEB. REV. STAT. § 28-638 (2010)
    - *See* State v. Babbitt, 762 N.W.2d 58 (Neb. 2009)
- *Unauthorized Computer Access*
  - NEB. REV. STAT. § 28-1343.01 (2010)
    - *See* Ervin & Smith Adver. and Pub. Relations, Inc. v. Ervin, No. 8:08CV459, 2009 WL 249998 (D. Neb. Feb. 3, 2009)
- *Depriving or Obtaining Property or Services*
  - NEB. REV. STAT. § 28-1344 (2010)
    - *See* Ervin & Smith Adver. and Pub. Relations, Inc. v. Ervin, No. 8:08CV459, 2009 WL 249998 (D. Neb. Feb. 3, 2009)
- *Harming or Disrupting Operations*
  - NEB. REV. STAT. § 28-1345 (2010)
    - *See* Ervin & Smith Adver. and Pub. Relations, Inc. v. Ervin, No. 8:08CV459, 2009 WL 249998 (D. Neb. Feb. 3, 2009)
- *Obtaining Confidential Public Information*
  - NEB. REV. STAT. § 28-1346 (2010)
- *Acts Without or Exceeding Authorization*
  - NEB. REV. STAT. § 28-1347 (2010)
    - *See* Ervin & Smith Adver. and Pub. Relations, Inc. v. Ervin, No. 8:08CV459, 2009 WL 249998 (D. Neb. Feb. 3, 2009)
- *Trade Secrets Act*
  - NEB. REV. STAT. §§ 87-501 to -507 (2010)
    - *See* Radiology Serv., P.C. v. Hall, 780 N.W.2d 17 (Neb. 2010); Magistro v. J. Lou, Inc., 703 N.W.2d 887 (Neb. 2005)
- *Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006*
  - NEB. REV. STAT. §§ 87-801 to -807 (2010)
- *Pending Legislation*
  - None

Nevada

- *Liability of Persons Who Transmit Items of Electronic Mail That Include Advertisements*
  - NEV. REV. STAT. §§ 41.705 to .735 (2010)
    - *See* Edwards v. Osteopathic Med. Assocs. of Nev., No. A468205, 2004 WL 5136225 (D. Nev. Mar. 5 2004)
- *Unlawful Acts Regarding Personal Identifying Information*
  - NEV. REV. STAT. §§ 205.461 to .4657 (2010)
- *Unlawful Acts jmnhb Computers and Information Services*
  - NEV. REV. STAT. §§ 205.473 to .513 (2010)
    - *See* Oracle USA, Inc. v. Rimini Street, Inc., No. 2:10-CV-00106-LRH-PAL, 2010 WL 3257933 (D. Nev. Aug. 13, 2010)
- *Unlawful Acts Involving Electronic Mail or Transmission of Other Data*

- NEV. REV. STAT. §§ 205.492, .511 to .513 (2010)
- *Uniform Trade Secrets Act*
  - NEV. REV. STAT. §§ 600A.010 to .100 (2010)
    - *See* Hutchison v. KFC Corp., 883 F. Supp. 517 (D. Nev. 1993); Menalco v. Buchan, No. 2:07-CV-01178-PMP-PA, 2010 WL 428911 (D. Nev.Feb. 1, 2010)
- *Trade Regulations and Practices: Computers*
  - NEV. REV. STAT. §§ 603.010 to .090 (2010)
    - *See* Menalco v. Buchan, 2010 WL 428911 (D. Nev. 2010)
- *Security of Personal Information*
  - NEV. REV. STAT. §§ 603A.010 to .920 (2010)
- *Pending Legislation*
  - None

New Hampshire

- *Uniform Trade Secrets Act*
  - N. H. STAT. ANN. §§ 350-B:1 to :9 (2010)
    - *See* Mortgage Specialists, Inc. v. Davey, 904 A.2d 652 (N.H. 2006); Anderson v. Century Prod. Co., 943 F. Supp. 137 (D. N.H 1996)
- *Notification of Security Breach Required*
  - N. H. STAT. ANN. §§ 359-C:19 to :21 (2010)
- *Computer Spyware*
  - N. H. STAT. ANN. §§ 359-H:1 to :6 (2010)
- *Identity Theft*
  - N. H. STAT. ANN. §§ 359-I:1 to :4 (2010)
- *Computer Crime*
  - N. H. STAT. ANN. §§ 638:16 to :19 (2010)
- *Identity Fraud*
  - N. H. STAT. ANN. § 638:26 (2010)
- *Pending Legislation*
  - None

New Jersey

- *Computer-Related Offenses: Civil Remedies*
  - N. J. STAT. ANN. § 2A:38A-3 (West 2010)
    - *See* Fairway Dodge, L.L.C. v. Decker Dodge Inc., 924 A.2d 517 (2007).
- *Trade Secrets Defined*
  - N.J. STAT. ANN. § 2C:20-1(i) (West 2010)
    - New Jersey does not currently have a statute governing trade secrets, such as the uniform provisions adopted by most other states. Instead, it bases its trade secrets doctrine on the common law.
      - *See* P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, L.L.C., 428 F.3d 504 (3d Cir. 2005).

- *Offenses Involving Access Device*
  - N. J. STAT. ANN. § 2C:20-1.1 (West 2010)
- *Computer-Related Crimes*
  - N. J. STAT. §§ 2C: 20-23 to -37 (West 2010)
    - This statutory section includes:
      - *Computer-Related Theft*
        - N. J. STAT. §§ 2C: 20-25 (West 2010)
          - *See* State v. Gaikwad, 793 A.2d 39 (N.J. Super. Ct. App. Div. 2002); State v. Riley, 988 A.2d 1252 (N.J. Super. Ct. Law Div. 2009)
      - *Wrongful Access, Disclosure of Information*
        - N. J. STAT. ANN. § 2C: 20-31 (West 2010)
          - State v. Riley, 988 A.2d 1252 (N.J. Super. Ct. Law Div. 2009)
      - *Obtaining, Copying, Accessing Program, Software Valued at $1,000 or Less*
        - N.J. STAT. ANN. § 2C:20-33 (West 2010)
          - *See* State v. Gaikwad, 793 A.2d 39 (N.J. Super. Ct. App. Div. 2002); State v. Riley, 988 A.2d 1252 (N.J. Super. Ct. Law Div. 2009)
- *Impersonation/Theft of Identity*
  - N.J. STAT. ANN. §§ 2C:21-17 to 17.6 (West 2010)
    - Piscitelli v. Classic Residence by Hyatt, 973 A.2d 948 (N.J. Super. Ct. App. Div. 2009)
      - This statutory scheme includes:
        - *Restitution to Victim of Unlawful Use of Personal Identifying Information*
          - N.J. STAT. ANN. § 2C:21-17.1 (West 2010)
        - *Use of Personal Identifying Information of Another*
          - N.J. STAT. ANN. § 2C:21-17.2 (West 2010)
        - *Other Identity Theft Related Provisions*
          - N.J. STAT. ANN. §§ 2C:21-17.3 to -17.6 (West 2010)
- *Disclosure of Breach of Security to Customers*
  - N.J. STAT. ANN. § 56:8-163 (West 2010)
- *Pending Legislation*
  - A175
    - According to the summary, the bill "[e]nhances duty and broadens liability concerning security of personal information, and response to breach of security, under 'Identity Theft Prevention Act.'"[282]
  - A921/S2456
    - New Jersey Trade Secrets Act[283]

[282] Bill available at http://www.njleg.state.nj.us/2010/Bills/A0500/175_I1.HTM.
[283] Bill available at http://www.njleg.state.nj.us/2010/Bills/A1000/921_I1.HTM.

- A1429
  - The summary states that the bill "[p]rohibits retail sales establishment from storing certain magnetic-stripe data; requires reimbursement for costs incurred by financial institution due to breach of security."[284]
- A1922
  - New Jersey Spam Deterrence Act[285]
- A2999
  - Requires payment of certain attorney's fees, expenses and costs in identity theft cases and adds debit card numbers to the definition of "personal identifying information."[286]

New Mexico

- *Theft of Identity: Obtaining Identity by Electronic Fraud*
  - N. M. STAT. § 30-16-24.1 (2010)
- *Computer Crimes Act*
  - N. M. STAT. § 30-45-1 to -7 (2010)
    - *See* State v. Rowell, 908 P.2d 1379 (N.M. 1995)
- *Uniform Trade Secrets Act*
  - N. M. STAT. §§ 57-3A-1 to -7 (2010)
    - *See* Pincheira v. Allstate Ins. Co., 190 P.3d 322 (N.M. 2008); Rapid Temps, Inc. v. Lamon, 192 P.3d 799 (N.M. Ct. App. 2008)
- *Unsolicited Email*
  - N. M. STAT. §§ 57-12-23 to -24 (2010)
- New Mexico does not have a security breach notification law[287]
- *Pending Legislation*
  - None

New York

- *Anti-Phishing Act of 2006*
  - N.Y. GEN. BUS. LAW § 390-b (2010)
- *Notification of Unauthorized Acquisition of Private Information*
  - N.Y. GEN. BUS. LAW § 899-aa (2010)
- *Offenses Involving Computers*
  - N.Y. PENAL LAW §§ 156.00 to .50 (2010)
    - This Act includes:
      - *Unauthorized Use of a Computer*
        - N.Y. PENAL LAW § 156.05 (2010)
          - *See* People v. Klapper, 902 N.Y.S.2d 305 (N.Y. Crim. Ct. 2010); People v. Angeles, 687 N.Y.S.2d 884 (N.Y. Crim. Ct. 1999);

[284] Bill available at http://www.njleg.state.nj.us/2010/Bills/A1500/1429_I1.HTM.
[285] Bill available at http://www.njleg.state.nj.us/2010/Bills/A2000/1922_I1.HTM.
[286] Bill available at http://www.njleg.state.nj.us/2010/Bills/A3000/2999_I1.HTM.
[287] State Security Breach Notification Laws, *supra* note 267.

Lawrence v. State, 688 N.Y.S.2d 392 (N.Y. Ct. Cl. 1999)

- *Computer Trespass*
  - N.Y. PENAL LAW § 156.10 (2010)
- *Computer Tampering*
  - N.Y. PENAL LAW §§ 156.20 to .27 (2010)
- *Unlawful Duplication of Computer Related Material*
  - N.Y. PENAL LAW §§ 156.29 to .30 (2010)
    - *See* People v. Angeles, 687 N.Y.S.2d 884 (N.Y. Crim. Ct. 1999); People v. Garcia, 647 N.Y.S.2d 355 (N.Y. Co. Ct. 1996); People v. Katakam, 660 N.Y.S.2d 334 ((N.Y. Sup. Ct. 1997)
- *Criminal Possession of Computer Related Material*
  - N.Y. PENAL LAW § 156.35 (2010)
    - *See* People v. Angeles, 687 N.Y.S.2d 884 (N.Y. Crim. Ct. 1999); People v. Garcia, 647 N.Y.S.2d 355 (N.Y. Co. Ct. 1996); People v. Katakam, 660 N.Y.S.2d 334 ((N.Y. Sup. Ct. 1997)

- *Unlawful Use of Secret Scientific Material*
  - N.Y. PENAL LAW § 165.07 (2010)
    - *See* People v. Russo, 501 N.Y.S.2d 276 (N.Y. Co. Ct.1986)
- *Identity Theft*
  - N.Y. PENAL LAW §§ 190.77 to .84 (2010)
    - *See* Kudelko v. Dalessio, 829 N.Y.S.2d 839 (N.Y. Civ. Ct. 2006)
- *Internet Security and Privacy Act*
  - N.Y. STATE TECH. LAW §§ 201 to 208 (2010)
    - This Act includes:
      - *Security Breach Notification*
        - N.Y. STATE TECH. LAW § 208 (2010)
- *Pending Legislation*
  - A.B. 49, 2010-2011 Assem., Reg. Sess. (NY. 2011)
    - Creates the crime of the criminal sale of an internet domain name to a terrorist group.[288]
  - S.B. 714, 2010-2011 S., Reg. Sess. (NY. 2011)
    - Creates computer crimes and increases penalties for crimes committed with the aid of a computer; provides for civil remedies and penal sanctions in cases of internet pornography.[289]
  - S.B. 1102, 2010-2011 S., Reg. Sess. (NY. 2011)

[288] Bill available at http://assembly.state.ny.us/leg/?default_fld=&bn=A00049%09%09&Summary=Y&Actions=Y&Votes=Y&Memo=Y&Text=Y.

[289] Bill available at http://assembly.state.ny.us/leg/?default_fld=%0D%0A&bn=SB+714%09&Summary=Y&Actions=Y&Votes=Y&Memo=Y&Text=Y.

- Creates the Computer Security Act.[290]
- A.B. 1050, 2010-2011 Assem., Reg. Sess. (NY. 2011)
  - Adds medical and health insurance information to the of identity theft provisions.[291]

North Carolina

- *Damages for Computer Trespass*
  - N. C. GEN. STAT. § 1-539.2A (2010)
- *Identity Theft/Identity Theft Protection Act*
  - N. C. GEN. STAT. § 14-113.20, and 75-60 to -66 (2010)
    - *See* State v. Dammons, 583 S.E.2d 606 (N.C. App. 2003); State v. Barron, 690 S.E.2d 22 (N.C. App. 2010)
      - The Identity Theft Protection Act Includes
        - *Protection from Security Breaches*
          - N. C. GENERAL STAT. § 75-65 (2010)
- *Computer-Related Crimes*
  - This statutory scheme includes:
    - *Accessing Computers/Government Computers*
      - N. C. GEN. STAT. §§ 14-454 to -454.1 (2010)
    - *Damaging Computers, Computer Programs, Computer Systems, Computer Networks, and Resources*
      - N. C. GEN. STAT. § 14-455 (2010)
        - *See* State v. Johnston, 618 S.E.2d 807 (N.C. Ct. App. 2005)
    - *Denial of Computer/Government Computer Services to an Authorized User*
      - N. C. GEN. STAT. §§ 14-456 to -456.1 (2010)
    - *Computer Extortion*
      - N. C. GEN. STAT. § 14-457 (2010)
    - *Computer Trespass*
      - N. C. GEN. STAT. § 14-458 (2010)
- *Trade Secrets Protection Act*
  - N. C. GEN. STAT. § 66-152 (2010)
    - *See* Philips Elec. N. Am. Corp. v. Hope, 631 F. Supp. 2d 705 (M.D. N.C. 2009); Merck & Co. Inc. v. Lyon, 941 F. Supp. 1443 (M.D. N.C. 1996); Barr-Mullin, Inc. v. Browning, 424 S.E.2d 226 (N.C. Ct. App. 1993)
- *Pending Legislation*
  - None

[290] Bill available at http://assembly.state.ny.us/leg/?default_fld=%0D%0A&bn=SB+1102%09&Summary=Y&Actions=Y&Votes=Y&Memo=Y&Text=Y.

[291] Bill available at http://assembly.state.ny.us/leg/?default_fld=%0D%0A&bn=AB+1050%09%09&Summary=Y&Actions=Y&Votes=Y&Memo=Y&Text=Y.

North Dakota

- *Computer Fraud/Computer Crime*
  - N. D. CENT. CODE § 12.1-06.1-08 (2010)
- *Unauthorized Use of Personal Identifying Information*
  - N.D. CENT. CODE § 12.1-23-11 (2010)
- *Uniform Trade Secrets Act*
  - N. D. CENT. CODE §12.1-06 47-25.1-01 to -08 (2010)
    - *See* Macquarie Bank Ltd. v. Knickel, 723 F. Supp. 2d 1161 (D. N.D. 2010); N. States Power Co. v. North Dakota Pub. Serv. Com'n, 502 N.W.2d 240 (N.D. 1993)
- *Commercial Electronic Mail Consumer Protection*
  - N.D. CENT. CODE §§ 51-27-01 to -10 (2010)
- *Notice of Security Breach for Personal Information*
  - N.D. CENT. CODE §§ 51-30-01 to -07 (2010)
- *Identity Fraud*
  - N.D. CENT. CODE §§ 51-31-01 to -05 (2010)
- *Pending Legislation*
  - None

Ohio

- *Uniform Trade Secrets Act*
  - OHIO REV. CODE ANN. §§ 1333.61 to .69 (2010)
    - *See* Asahi Glass Co., Ltd. v. Toledo Eng'g Co., Inc., 505 F. Supp. 2d 423 (N.D. Ohio 2007); Alpha Benefits Agency, Inc. v. King Ins. Agency, Inc., 731 N.E.2d 1209 (Ohio Ct. App. 1999)
- *Disclosure of Security Breach of Computerized Personal Information Data*
  - OHIO REV. CODE ANN. §§ 1347.12, 1349.19 to .192 (2010)
- *Regulating Electronic Mail Advertisements*
  - OHIO REV. CODE ANN. § 2307.64 (2010)
    - *Recognized as Preempted by* Ferron v. EchoStar Satellite, LLC, No. 2:06-CV-00453, 2009 WL 6700648 (S.D. Ohio Sept. 29, 2009)
- *Computer Crimes*
  - OHIO REV. CODE ANN. § 2909.07(A)(6) (2010)
- *Unauthorized Use of Property - Computer, Cable, or Telecommunication Property*
  - OHIO REV. CODE ANN. § 2913.04 (2010)
    - *See* State v. Mason, 757 N.E.2d 789 (Ohio Ct. App. 2001); State v. Washington, 710 N.E.2d 307 (Ohio Ct. App. 1998); Universal Tube & Rollform Equip. Corp. v. YouTube, Inc., 504 F. Supp. 2d 260 (N.D. Ohio 2007)
- *Illegally Transmitting Multiple Commercial Electronic Mail Messages (Spamming) - Unauthorized Access of Computer*
  - OHIO REV. CODE ANN. § 2913.421 (2010)
- *Identity Fraud*
  - OHIO REV. CODE ANN. § 2913.49 (2010)

        - *See* State v. Ladson, No. 85709, 2005 WL 2467059 (Ohio Ct. App. Oct. 6, 2005)
- *Pending Legislation*
    - None

Oklahoma

- *Fraudulent Electronic Mail Messages*
    - OKLA. STAT. tit. 15, §§ 776.1 to .7 (2010)
        - *Recognized as preempted by CAN-SPAM Act in* Omega World Travel, Inc. v. Mummagraphics, Inc., 469 F.3d 348, 350 (4th Cir. 2006)
- *Anti-Phishing Act*
    - OKLA. STAT. tit. 15, §§ 776.8 to .12 (2010)
- *Identity Theft*
    - OKLA. STAT. tit. 21, § 1533.1 (2010)
- *Oklahoma Computer Crimes Act*
    - OKLA. STAT. tit. 21, §§ 1951 to -58 (2010)
        - *See* Davis v. State, 916 P.2d 251 (Okl. Crim. App. 1996)
- *Security Breach Notification Act*
    - OKLA. STAT. tit. 24, § 161 (2010)
- *Disclosure of Breach of Security of Computerized Personal Information*
    - OKLA. STAT. tit. 74, § 3113.1 (2010)
- *Uniform Trade Secrets Act*
    - OKLA. STAT. tit. 78, §§ 85 to 94 (2010)
        - *See* Micro Consulting, Inc. v. Zubeldia, 813 F. Supp. 1514 (W.D. Okl.1990)
- *Pending Legislation*
    - None

Oregon

- *Computer Crime*
    - OR. REV. STAT. § 164.377 (2010)
        - *See* State v. Schwartz, 21 P.3d 1128 (Or. Ct. App. 2001)
- *Identity Theft*
    - OR. REV. STAT. § 165.800 (2010)
        - *See* State v. Porter, 108 P.3d 107 (Or. Ct. App. 2005)
- *Uniform Trade Secrets Act*
    - OR. REV. STAT. §§ 646.461 to .475 (2010)
        - *See* Acrymed, Inc. v. Convatec, 317 F. Supp. 2d 1204 (D. Or. 2004); IKON Office Solutions, Inc. v. Am. Office Prod., Inc., 178 F. Supp. 2d 1154 (D. Or. 2001)
- *Notice of Breach of Security*
    - OR. REV. STAT. § 646A.604 (2010)
- *Anti-Spam Legislation*
    - Act of Sept. 17, 2003, 2003 Or. Laws 759
- *Pending Legislation*

- None

Pennsylvania

- *Uniform Trade Secrets Act*
  - 12 PA. CONS. STAT. §§ 5301-5308 (2010)
    - *See* Fishkin v. Susquehanna Partners, G.P., 340 F. App'x. 110, 118 (3d Cir. 2009); The Bancorp Bank. v. Isaacs, No. 07-CV-1907, 2010 WL 1141336 (E.D. Pa. Mar. 25, 2010)
- *Identity Theft*
  - 18 PA. CONS. STAT. § 4120 (2010)
    - See Com. v. Newton, 994 A.2d 1127 (Pa. Super. Ct. 2010)
- *Computer Offenses*
  - 18 PA. CONS. STAT. §§ 7601-7661 (2010)
    - This Act includes:
      - *Hacking and Similar Offenses*
        - 18 PA. CONS. STAT. §§ 7611-7616 (2010)
          - *See* Com. v. Delapaz, 796 A.2d 364 (Pa. Super. Ct. 2002); Bowman v. Burroughs, No. 07-185, 2008 WL 5427910 (W.D. Pa. Dec. 30, 2008)
      - *Unlawful Transmission of Electronic Mail*
        - 18 PA. CONS. STAT. § 7661 (2010)
- *Unsolicited Telecommunication Advertisement Act*
  - 73 PA. STAT. ANN. §§ 2250.1 to .8 (West 2010)
    - Included within this act are:
      - *Prohibition of Unsolicited or Misleading Commercial Electronic Mail Messages and Faxes*
        - 73 PA. STAT. ANN. § 2250.3 (West 2010)
      - *Other Conduct*
        - 73 PA. STAT. ANN. § 2250.4 (West 2010)
      - *Blocking of Commercial Electronic Mail*
        - 73 PA. STAT. ANN. § 2250.6 (West 2010)
          - *See* Aronson v. VMT Scientific, No. 06-000002, 2006 WL 3192257 (Pa. Com. Pl. July 22, 2006)
- *Notification of Breach*
  - 73 PA. STAT. ANN. § 2303 (West 2010)
- *Pending Legislation*
  - H.B. 2605 (2010 Legislative Session)
    - Provides for immunity for private colleges for security breaches involving student data or records shared with the Department of Education.[292]

[292] Bill available at http://www.legis.state.pa.us/cfdocs/legis/PN/Public/btCheck.cfm?txtType=HTM&sessYr=2009&sessInd=0&billBody=H&billTyp=B&billNbr=2605&pn=4036.

Rhode Island

- *Uniform Trade Secrets Act*
  - R.I. GEN. LAWS §§ 6-41-1 to -11 (2010)
    - *See* Magnum Defense, Inc. v. Harbour Group Ltd., 248 F. Supp. 2d 64 (D. R.I. 2003); Astro-Med, Inc. v. Nihon Kohden America, Inc., 591 F.3d 1 (1st Cir. 2009); APG, Inc. v. MCI Telecomm. Corp., 436 F.3d 294 (1st Cir. 2006)
- *Unsolicited Electronic Mail*
  - R.I. GEN. LAWS § 6-47-2 (2010)
- *Electronic Mail Fraud Regulatory Act*
  - R.I. GEN. LAWS §§ 6-49-1 to -6 (2010)
- *Impersonation and Identity Fraud Act*
  - R.I. GEN. LAWS §§11-49.1-1 to -5 (2010)
- *Notification of Breach*
  - R.I. GEN. LAWS § 11-49.2-3 (2010)
- *Computer Crime*
  - R. I. GEN. LAWS §§ 11-52-1 to -8 (2010)
    - *This statute includes:*
      - *Access to Computer for Fraudulent Purpose*
        - R. I. GEN. LAWS § 11-52-2 (2010)
      - *Intentional Access, Alteration, Damage, or Destruction*
        - R. I. GEN. LAWS § 11-52-3 (2010)
          - *See* Wilson v. Moreau, 440 F. Supp. 2d 81 (D. R.I. 2006); Chain Store Maint., Inc. v. Nat'l Glass & Gate Serv., Inc., No. Civ.A. PB 01-3522, 2004 WL 877599 (R.I. Super. Ct. Apr. 21, 2004)
      - *Computer Theft*
        - R. I. GEN. LAWS § 11-52-4 (2010)
          - *See* Chain Store Maint., Inc. v. Nat'l Glass & Gate Serv., Inc., No. Civ.A. PB 01-3522, 2004 WL 877599 (R.I. Super. Ct. Apr. 21, 2004)
      - *Computer Trespass*
        - R. I. GEN. LAWS § 11-52-4.1 (2010)
          - *See* Wilson v. Moreau, 440 F. Supp. 2d 81 (D. R.I. 2006)
      - *Civil Action*
        - R. I. GEN. LAWS § 11-52-6 (2010)
          - *See* Wilson v. Moreau, 440 F. Supp. 2d 81 (D. R.I. 2006)
      - *Use of False Information*
        - R. I. GEN. LAWS § 11-52-7 (2010)
      - *Tampering with Computer Source Documents*
        - R. I. GEN. LAWS § 11-52-8 (2010)
- *Internet Misrepresentation of Business Affiliation Act*

- R. I. GEN. LAWS §§ 11-52.1-1 to -5 (2010)
- *Software Fraud*
  - R. I. GEN. LAWS §§ 11-52.2-1 to -8 (2010)
- *Online Property Offenses*
  - R. I. GEN. LAWS §§ 11-52.3-1 to -5 (2010)
- *Pending Legislation*
  - None

South Carolina

- *Personal Financial Security Act*
  - S.C. CODE ANN. §§ 16-13-500 to -530 (2010)
- *Computer Crime Act*
  - S.C. CODE ANN. §§ 16-16-10 to -40 (2010)
    - *See* Jennings v. Jennings, 697 S.E.2d 671 (S.C. Ct. App. 2010)
- *Consumer Identity Theft Protection*
  - S.C. CODE ANN. §§ 37-20-110 to -200 (2010)
- *Breach of Security of Business Data*
  - S.C. CODE ANN. § 39-1-90 (2010)
- *South Carolina Trade Secrets Act*
  - S.C. CODE ANN. §§ 39-8-10 to -130 (2010)
    - *See* Jackson v. Honda of South Carolina Mfg., Inc., No. 4:03-3459, 2006 WL 2780959 (D. S.C. Sept. 25, 2006); Laffitte v. Bridgestone Corp., 674 S.E.2d 154 (S.C. 2009)
- *Pending Legislation*
  - H.B. 3213
    - Amends the Computer Crimes Act to include that it is unlawful for a person to directly or indirectly access a computer or network without proper authorization with the purpose of obtaining and releasing state or federal classified or confidential information to the public.[293]

South Dakota

- *Identity Theft*
  - S.D. CODIFIED LAWS § 22-40-8 (2010).
- *Spam E-mail*
  - S.D. CODIFIED LAWS §§ 37-24-42 to -48 (2010)
- *Uniform Trade Secrets Act*
  - S.D. CODIFIED LAWS §§ 37-29-1 to -11 (2010)
    - *See* Paint Brush Corp., Parts Brush Div. v. Neu, 599 N.W.2d 384 (S.D. 1999); Daktronics, Inc. v. McAfee, 599 N.W.2d 358 (S.D. 1999)
- *Unlawful Uses of Computer System*
  - S.D. CODIFIED LAWS §§ 43-43B-1 to -8 (2010).

[293] Bill available at http://www.scstatehouse.gov/cgi-bin/query.exe?first=DOC&querytext=internet&category=Legislation&session=119&conid=6124955&result_pos=20&keyval=1193213.

- South Dakota does not have a security breach law[294]
- *Pending Legislation*
    - None

Tennessee

- *Identity Theft Victims' Rights Act of 2004*
    - TENN. CODE ANN. § 39-14-150 (2010)
        - *See* U.S. v. Johnson, 356 F. App'x. 785 (6th Cir. 2009); State v. Herron, No. W2009-02493-CCA-R3-CD, 2010 WL 4674260 (Tenn. Crim. App. Aug. 3, 2010)
- *Tennessee Personal and Commercial Computer Act of 2003*
    - TENN. CODE ANN. §§ 39-14-601 to -606 (2010)
        - *See* State v. Joyner, 759 S.W.2d 422 (Tenn. Crim. App. 1987); Fleming v. Xerox Connect, Inc., 50 F. App'x. 211 (6th Cir. 2002); Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929 (W.D. Tenn. 2008)
- *Tennessee Identity Theft Deterrence Act of 1999*
    - TENN. CODE ANN. §§ 47-18-2101 to -2110 (2010)
        - This Act includes:
            - *Release of Personal Consumer Information*
                - TENN. CODE ANN. § 47-18-2107 (2010)
                    - *See* Walton v. Nova Info. Sys., No. 3:06-CV-292, 2008 WL 1751525 (E.D. Tenn. Apr. 11, 2008); Wolfe v. MBNA America Bank, 485 F. Supp. 2d 874 (W.D. Tenn. 2007)
- *Unsolicited Advertising by Electronic Means*
    - TENN. CODE ANN. §§ 47-18-2501 to -2502 (2010)
        - *See* Beam Miller & Rogers PLLC v. OfficePlanner, Inc., No. 02C-1598, 2002 WL 34185324 (Tenn. Cir. Ct. Dec. 4, 2002)
- *Anti-Phishing Act of 2006*
    - TENN. CODE ANN. §§ 47-18-5201 to -5205 (2010)
- *The Uniform Trade Secrets Act*
    - TENN. CODE ANN. §§ 47-25-1701 to -1709 (2010)
        - *See* Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967 (M.D. Tenn. 2008); Stratienko v. Cordis Corp., 429 F.3d 592 (6th Cir. 2005)
- *Pending Legislation*
    - None

Texas

- *Regulation of Certain Electronic Email*
    - TEX. BUS. & COM. CODE ANN. §§ 321.001 to .114 (Vernon 2010)
- *Consumer Protection Against Computer Spyware Act*
    - TEX. BUS. & COM. CODE ANN. §§ 324.001 to .102 (Vernon 2010)

[294]State Security Breach Notification Laws, *supra* note 267.

- *Internet Fraud: Anti-Phishing Act*
  - TEX. BUS. & COM. CODE ANN. §§ 325.001 to .006 (Vernon 2010)
- *Identity Theft Enforcement and Protection Act*
  - TEX. BUS. & COM. CODE ANN. §§ 521.001 to .152 (Vernon 2010)
    - The Act includes:
      - *Unauthorized Use or Possession of Personal Identifying Information*
        - TEX. BUS. & COM. CODE ANN. § 521.051 (Vernon 2010)
      - *Notification Required Following Breach of Security of Computerized Data*
        - TEX. BUS. & COM. CODE ANN. § 521.053 (Vernon 2010)
- *Unlawful Access to Stored Communications*
  - TEX. PENAL CODE ANN. § 16.04 (Vernon 2010)
- *Theft of Trade Secrets*
  - TEX. PENAL CODE ANN. § 31.05 (Vernon 2010)
    - *See* In re Cooper Tire & Rubber Co., 313 S.W.3d 910 (Tex. App. 2010); IBP, Inc. v. Klumpe, 101 S.W.3d 461 (Tex. App. 2001)
- *Fraudulent Use or Possession of Identifying Information*
  - TEX. PENAL CODE ANN. § 32.51 (Vernon 2010)
    - *See* Richardson v. State, No. 2-09-195-CR, 2010 WL 3193558 (Tex. App. Aug. 12, 2010); Ford v. State, 282 S.W.3d 256, 257 (Tex. App. 2009); Long v. State, 245 S.W.3d 563 (Tex. App. 2007)
- *Computer Crimes*
  - TEX. PENAL CODE ANN. §§ 33.01 to .07 (Vernon 2010)
    - *See* Signorelli v. State, No. 09-06-450 CR, 2007 WL 4723210 (Tex. App. Apr. 23, 2008); Mitchell v. State, 12 S.W.3d 158 (Tex. App. 2000)
- *Pending Legislation*
  - None

Utah

- *Uniform Trade Secrets Act*
  - UTAH CODE ANN. §§ 13-24-1 to -9 (2010)
    - *See* Russo v. Ballard Med. Prod., 550 F.3d 1004 (10th Cir. 2008); ClearOne Communc'n, Inc. v. Chiang, 608 F. Supp. 2d 1270, 1277 (D. Utah Apr. 09, 2009)
- *Utah E-Commerce Integrity Act*
  - UTAH CODE ANN. §§ 13-40-101 to -402 (2010)
    - Included in the E-commerce Act are:
      - *Phishing and Pharming*
        - UTAH CODE ANN. § 13-40-201 (2010)
          - *Prior Version Recognized as Unconstitutional by* Overstock.com, Inc. v.

SmartBargains, Inc., 192 P.3d 858 (Utah 2008)

- *Removal of Domain Name or Content*
  - UTAH CODE ANN. § 13-40-202 (2010)
    - *See id.*
- *Spyware Protection*
  - UTAH CODE ANN. §§ 13-40-301 to -303 (2010)
    - *See id.*
- *Enforcement*
  - UTAH CODE ANN. §§ 13-40-401 to -402 (2010)
    - *See id.*

- *Protection of Personal Information Act*
  - UTAH CODE ANN. §§ 13-44-101 to -301 (2010)
- *Computer Crimes Act*
  - UTAH CODE ANN. §§ 76-6-701 to -705 (2010)
    - *See* State v. Kent, 945 P.2d 145 (Utah Ct. App. 1997)
- *Identity Fraud*
  - UTAH CODE ANN. §§ 76-6-1101 to 1105 (2010)
    - *See* State v. Valdez, 78 P.3d 627 (Utah Ct. App. 2003); State v. Chukes, 71 P.3d 624 (Utah Ct. App. 2003); United States v. Johnson, 584 F.3d 995 (10th Cir. 2009)
- *Pending Legislation*
  - None

Vermont

- *Protection of Personal Information*
  - VT. STAT. ANN. tit. 9, § 2435 (2010)
- *Identity Theft*
  - Vt. Stat. Ann. tit. 13, § 2030 (2010)
- *Computer Crimes*
  - VT. STAT. ANN. tit. 13, §§ 4101-07 (2010)
    - Computer Crimes statute includes:
      - *Unauthorized Access*
        - VT. STAT. ANN. tit. 13, § 4102 (2010)
      - *Access to Computer for Fraudulent Purposes*
        - VT. STAT. ANN. tit. 13, § 4103 (2010)
      - *Alteration, Damage, or Interference*
        - VT. STAT. ANN. §tit. 13, § 4104 (2010)
      - *Theft or Destruction*
        - VT. STAT. ANN. tit. 13, § 4105 (2010)
      - *Civil Liability*
        - VT. STAT. ANN. tit. 13, § 4106 (2010)
- *Trade Secrets*
  - VT. STAT. ANN. tit. 9, §§ 4601-09 (2010)
    - *See* Dicks v. Jensen, 768 A.2d 1279 (Vt. 2001); Vermont Microsystems, Inc. v. Autodesk, Inc., 88 F.3d 142 (2d Cir.1996);

Omega Optical, Inc. v. Chroma Tech. Corp., 800 A.2d 1064 (Vt. 2002)

- *Pending Legislation*
  - None

Virginia

- *When Personal Jurisdiction Over Person May be Exercised*
  - VA. CODE ANN. § 8.01-328.1(B) (2010)
- *Virginia Computer Crimes Act*
  - VA. CODE ANN. §§ 18.2-152.1 to .15 (2010)
    - Included within the Computer Crimes Act are:
      - *Computer Fraud*
        - VA. CODE ANN. § 18.2-152.3 (2010)
          - *Preempted by* SecureInfo Corp. v. Telos Corp., 387 F. Supp. 2d 593 (E.D. Va. 2005)
      - *Transmission of unsolicited commercial electronic mail (spam)*
        - VA. CODE ANN. §§ 18.2-152.3:1 (2010)
          - *Prior Version Held Unconstitutional by* Jaynes v. Com., 666 S.E.2d 303 (Va. 2008)
      - *Computer Trespass*
        - VA. CODE ANN. § 18.2-152.4 (2010)
          - *See* Verizon Online Serv., Inc. v. Ralsky, 203 F. Supp. 2d 601 (E.D. Va. 2002)
      - *Computer Invasion of Privacy*
        - VA. CODE ANN. § 18.2-152.5 (2010)
          - *See* Global Policy Partners, LLC v. Yessin, 686 F. Supp. 2d 631 (E.D. Va. 2009); Plasters v. Com., No. 1870-99-3, 2000 WL 827940 (Va. Ct. App. June 27, 2000)
      - *Using a Computer to Gather Identifying Information*
        - VA. CODE ANN. §§ 18.2-152.5:1 (2010)
      - *Theft of Computer Services*
        - VA. CODE ANN. § 18.2-152.6 (2010)
          - *See* A.V. v. iParadigms, Ltd. Liab. Co., 544 F. Supp. 2d 473 (E.D. Va. 2008), *aff'd in part, rev'd in part*, A.V. ex rel. Vanderhye v. iParadigms, LLC, 562 F.3d 630 (4th Cir. 2009)
      - *Personal Trespass by Computer*
        - VA. CODE ANN. § 18.2-152.7 (2010)
          - *See* Saks Fifth Avenue, Inc. v. James, Ltd., 630 S.E.2d 304, 308 (Va. 2006)
      - *Harassment by Computer*
        - VA. CODE ANN. § 18.2-152.7:1 (2010)

- *See* Miller v. Washington Workplace, Inc., 298 F. Supp. 2d 364 (E.D. Va. 2004); Airhart v. Com, No. 1219-05-2, 2007 WL 88747 (Va. Ct. App. Jan. 16, 2007)
- *Computer as Instrument of Forgery*
  - VA. CODE ANN. § 18.2-152.14 (2010)
    - *See* Com. v. Bechtler, No. 23759, 2001 WL 803451 (Va. Cir. Ct. May 25, 2001); America Online, Inc. v. Smith, No. Civ.A.05-0344, 2006 WL 181674 (E.D. Va. Jan. 24, 2006)
- *Encryption Used in Criminal Activity*
  - VA. CODE ANN. § 18.2-152.15 (2010)

- *Identity Theft*
  - VA. CODE ANN. § 18.2-186.3 (2010)
    - *See* Gheorghiu v. Com., 682 S.E.2d 50 (Va. Ct. App. 2009), *aff'd in part, rev'd in part*, 701 S.E.2d 407 (Va. 2010)
- *Identity Fraud*
  - VA. CODE ANN. § 18.2-186.3:1 (2010)
- *Breach of Personal Information Notification*
  - VA. CODE ANN. § 18.2-186.6 (2010)
- *Venue for Prosecution of Computer Crimes*
  - VA. CODE ANN. § 19.2-249.2 (2010)
    - *See* Barson v. Com., No. 2464-09-1, 2010 WL 4284631 (Va. Ct. App. Nov. 2, 2010)
- *Breach of Medical Information Notification*
  - VA. CODE ANN. § 32.1-127.1:05 (2010)
    - Effective January 1, 2011.
- *Uniform Trade Secrets Act*
  - VA. CODE ANN. §§ 59.1-336 to -343 (2010)
    - *See* MicroStrategy Inc. v. Li, 601 S.E.2d 580 (Va. 2004)
- *Pending Legislation*
  - H.B. 1207 (Continued to 2011 in Senate Finance Committee)
    - Expands computer trespass to include, in certain situations, the use of video and image capture software or hardware in addition to keystroke loggers.[295]

Washington

- *Identity Crimes*
  - WASH. REV. CODE. ANN. §§ 9.35.001 to .902 (2010)
    - This statutory scheme includes:
      - *Identity Theft*
        - WASH. REV. CODE. ANN. § 9.35.020 (2010)

[295]Bill available at http://leg1.state.va.us/cgi-bin/legp504.exe?ses=111&typ=bil&val=hb1207.

- *See* State v. Fisher, 161 P.3d 1054 (Wash. Ct. App. 2007); State v. Baldwin, 45 P.3d 1093 (Wash. Ct. App. 2002)

- *Computer Trespass*
  - WASH. REV. CODE. ANN. §§ 9A.52.110 to .130 (2010)
    - *See* State v. Riley, 846 P.2d 1365 (Wash. 1993); State v. Olson, 735 P.2d 1362 (Wash. Ct. App. 1987)
- *Uniform Trade Secrets*
  - WASH. REV. CODE. ANN. §§ 19.108.010 to .940 (2010)
    - *See* Pac. Aerospace & Elec., Inc. v. Taylor, 295 F. Supp. 2d 1205 (E.D. Wash. 2003); Ed Nowogroski Ins., Inc. v. Rucker, 971 P.2d 936 (Wash. 1999); Thola v. Henschell, 164 P.3d 524 (Wash. Ct. App. 2007); Ultimate Timing, L.L.C. v. Simms, 715 F. Supp. 2d 1195 (W.D. Wash. 2010); McCallum v. Allstate Prop. & Cas. Ins. Co., 204 P.3d 944 (Wash. Ct. App. 2009)
- *Commercial Electronic Mail*
  - WASH. REV. CODE. ANN. §§ 19.190.010 to .110 (2010)
    - *Preempted by CAN-SPAM Act in* Ferguson v. Active Response Group, 348 F. App'x. 255 (9th Cir. 2009); State v. Heckel, 93 P.3d 189, 189 (Wash. Ct. App. 2004); Gordon v. Impulse Mktg. Group, Inc., 375 F. Supp. 2d 1040 (E.D. Wash. 2005); Benson v. Oregon Processing Serv., Inc., 150 P.3d 154 (Wash. Ct. App. 2007)
- *Personal Information-Notice of Security Breaches*
  - WASH. REV. CODE. ANN. §§19.255.010 to .20, 42.56.590 (2010)
- *Computer Spyware*
  - WASH. REV. CODE. ANN. §§19.270.010 to .900 (2010)
    - *See* Johnson v. Microsoft Corp., No. C06-0900RAJ, 2009 WL 1794400 (W.D. Wash. June 23, 2009); State v. Securelink Networks, LLC, No. 07-2-04987-8 SEA, 2008 WL 2164222 (Wash. Super. Ct. May 20, 2008)
- *Pending Legislation*
  - None

West Virginia

- *Breach of Security of Consumer Information*
  - W. VA. CODE §§ 46A-2A-101 to -105 (2010)
- *Electronic Mail Protection Act*
  - W. VA. CODE §§ 46A-6G-1 to -5 (2010)
- *Uniform Trade Secrets Act*
  - W. VA. CODE §§ 47-22-1 to -10 (2010)
    - *See* IVS Hydro, Inc. v. Robinson, 93 F. App'x. 521 (4th Cir. 2004); McGough v. Nalco Co., 496 F. Supp. 2d 729 (N.D. W.Va. 2007)
- *West Virginia Computer Crime and Abuse Act*
  - W. VA. CODE §§ 61-3C-1 to -21 (2010)
    - Included in the Computer Crime and Abuse Act are:

- *Computer Fraud/Access to Legislature Computer*
  - W. VA. CODE § 61-3C-4 (2010)
- *Unauthorized Access to Computer Services*
  - W. VA. CODE § 61-3C-5 (2010)
- *Unauthorized Possession of Computer Data or Programs*
  - W. VA. CODE § 61-3C-6 (2010)
- *Alteration/Destruction of Computer Equipment*
  - W. VA. CODE § 61-3C-7 (2010)
- *Disruption of Computer Services*
  - W. VA. CODE § 61-3C-8 (2010)
- *Unauthorized Possession of Computer Information*
  - W. VA. CODE § 61-3C-9 (2010)
- *Disclosure of Computer Security Information*
  - W. VA. CODE § 61-3C-10 (2010)
- *Obtaining Confidential Public Information*
  - W. VA. CODE § 61-3C-11 (2010)
- *Computer Invasion of Privacy*
  - W. VA. CODE § 61-3C-12 (2010)
    - *See* Lawyer Disciplinary Bd. v. Markins, 663 S.E.2d 614 (W.Va. 2008)
- *Fraud and Related Activity in Connection with Access Devices*
  - W. VA. CODE § 61-3C-13 (2010)
- *Endangering Public Safety*
  - W. VA. CODE § 61-3C-14 (2010)
- *Obscene, Anonymous, Harassing and Threatening Communications by Computer*
  - W. VA. CODE § 61-3C-14a (2010)
    - U.S. v. Testerman, No. CRIM.A. 1:05CR04, 2005 WL 1047556 (N.D. W.Va. Apr. 28, 2005)
- *Computer as Instrument of Forgery*
  - W. VA. CODE § 61-3C-15 (2010)
- *Civil Relief*
  - W. VA. CODE § 61-3C-16 (2010)

- *Taking Identity of Another Person*
  - W. VA. CODE § 61-3-54 (2010)
- *Pending Legislation*
  - None

Wisconsin

- *Uniform Trade Secrets Acts*
  - WISC. STAT. § 134.90 (2010)
    - *See* Metso Minerals Indus., Inc. v. FLSmidth-Excel LLC, No. 07-CV-926, 2010 WL 1850139 (E.D. Wis. May 7, 2010); Radiator Exp. Warehouse, Inc. v. Shie, 708 F. Supp. 2d 762 (E.D. Wis.

2010); Genzyme Corp. v. Bishop, 463 F. Supp. 2d 946 (W.D. Wis. 2006); World Wide Prosthetic Supply, Inc. v. Mikulsky, 631 N.W.2d 253 (Wis. Ct. App. 2001)

- *Notice of Unauthorized Acquisition of Personal Information*
  - WISC. STAT. § 134.98 (2010)
- *Computer Crimes*
  - WISC. STAT. § 943.70 (2010)
    - *See* State v. Corcoran, 522 N.W.2d 226 (Wis. Ct. App. 1994); Burbank Grease Serv., LLC v. Sokolowski, 717 N.W.2d 781 (Wis. 2006); Maxpower Corp. v. Abraham, 557 F. Supp. 2d 955 (W.D. Wis. 2008)
- *Unauthorized Use of an Individual's Personal Identifying Information or Documents*
  - WISC. STAT. § 943.201 (2010)
    - *See* State v. Baron 754 N.W.2d 175 (Wis. Ct. App. 2008), *aff'd* 769 N.W.2d 34 (Wis. 2009); State v. Lis, 751 N.W.2d 891 (Wis. Ct. App. 2008); State v. Ramirez, 633 N.W.2d 656 (Wis. Ct. App. 2001); State v. Peters, 665 N.W.2d 171 (Wis. 2003)
- *Unauthorized Use of an Entity's Identifying Information or Documents*
  - WISC. STAT. § 943.203 (2010)
- *Theft of Trade Secrets*
  - WISC. STAT. § 943.205 (2010)
    - *See* RTE Corp. v. Coatings, Inc., 267 N.W.2d 226 (Wis. 1978)
- *Sending Obscene or Sexually Explicit Electronic Messages*
  - WISC. STAT. § 944.25 (2010)
    - *See* State v. Weidner, 611 N.W.2d 684 (Wis. 2000)
- *Pending Legislation*
  - None

Wyoming

- *Computer Crimes*
  - WYO. STAT. ANN. §§ 6-3-501 to -505 (2010)
    - Computer Crimes include:
      - *Crimes Against Intellectual Property*
        - WYO. STAT. ANN. § 6-3-502 (2010)
      - *Crimes Against Computer Equipment or Supplies*
        - WYO. STAT. ANN. § 6-3-503 (2010)
      - *Crimes Against Computer Users*
        - WYO. STAT. ANN. § 6-3-504 (2010)
- *Theft of Identity*
  - WYO. STAT. ANN. § 6-3-901 (2010)
- *Commercial Electronic Mail*
  - WYO. STAT. ANN. §§ 40-12-401 to -404 (2010)
- *Computer Security Breach*
  - WYO. STAT. ANN. § 40-12-502 (2010)
- *Uniform Trade Secrets Act*

- WYO. STAT. ANN. §§ 40-24-101 to -110 (2010)

- *Pending Legislation*
  - None

V. CONCLUSION

¶ 66 Crime is a problem that is impossible to solve. It seems that our statutes and law enforcement measures have always been one step behind the criminals. These difficulties remain the same in the cyber realm, where cybersecurity "has been largely reactive in nature . . . ."[296] Indeed, "[l]aw enforcement resources in cyberspace cannot keep pace with sophisticated cybercrime subcultures in anonymous offshore havens."[297] Nevertheless, our government and the nation's businesses must take whatever steps possible to combat cybercrime. While the federal government has improved our nation's readiness, partisan politics appear to stand in the way of more comprehensive legislative reform in the near future. With the risk to our national security and economy so great, and with carefully coordinated attacks from foreign enemies on the rise, Congress must act to pass a comprehensive cybersecurity package without delay.

¶ 67 And from the business perspective, although the defensive cyber-measures taken by larger companies will necessarily be complex and expensive, every business owner should focus on creating a level of cyber-awareness amongst staff to reduce the company's potential exposure to cyber-attack. Simple measures such as creating robust passwords to internal systems, avoiding the use of web-based email while on unsecured networks, deleting and reporting spam messages, and tracking any "outlier" historical patterns which show unusual employee access to sensitive corporate data, can go a long way towards making any company more "cyber-secure." As best stated by noted cyber law attorney Renato Opice Blum,[298] "the reality is such that the profits from cybercrimes often surpass drug dealing, and the question now lies on which preventive and punitive measures should be taken. At a minimum, awareness and education are necessary to keep up with the pace of these criminals."

---

[296] GEORGIA TECH, *supra* note 50, at 2 (quoting Mustaque Ahamad, Director of the Georgia Tech Information Security Center).

[297] Rustad, *supra* note 27, at 66.

[298] Opice Blum Advogados Associados, http://www.opiceblum.com.br/lang-en/01_profissionais_dadosRes.php?ID_CUREQUIPE=138578 (last visited October 19, 2010).