ARTICLE:

CYBERCRIME: ISSUES AND CHALLENGES IN THE UNITED STATES

By **Chief Judge B. Lynn Winmill, David L. Metcalf and Michael E. Band**

Introduction

Computer historians remember Thomas Watson, the first chairman of IBM, for two famous quotes. The first was IBM's motto: "THINK". It became a commonly repeated word, being printed on the cover of notebooks, scratchpads, and even matchbooks. "THINK" magazine was distributed monthly to IBM employees.[1] In light of this high-minded credo, it is perhaps ironic that the second quote, for which Mr Watson is more notoriously remembered, is as follows:

> "I think there is a world market for maybe five computers."[2]

That attitude persisted in the industry for the next few decades. Even thirty-four years later in 1977, Ken Olson, the President of Digital Equipment Corp (the predecessor to Hewlett Packard and Compaq) is alleged to have remarked "There is no need for any individual to have a computer in their home." As absurd as these statements may seem today, history will forgive Messrs. Watson and Olson. These were men at the very forefront of their field and even they could not envisage the full scope of the revolution that they themselves were in the process of ushering in. Nor could they have imagined how rapidly the revolution would come.

In 1980, three years after Mr. Olson's remark, approximately twelve companies sold 724,000 computers worldwide. The following year, twenty more companies, including IBM, entered the market, and sales doubled to 1.4 million units. In 1982, *Time* magazine named the computer its 'Machine of the Year' and predicted that by year's end, more than 100 companies would sell 2.8 million personal computers.[3] Just like that, personal computing had grown from professional niche into a multi-billion dollar industry with no sign of slowing down.

Yet even as the computer revolution kicked into high gear, the dangers posed by the revolution were still being misapprehended. In the *Time* article proclaiming the computer "Machine of the Year," concerned experts laboured over the potential consequences that social assimilation of the computer might cause. Would the human brain stupefy as computers began making our decisions for us? Would assimilation of computers into society at large lead to the establishment of an "intellectual ruling class"? Professor Marvin Minsky of M.I.T. is quoted in the same *Time* article as stating that, "[t]he desktop revolution has brought the tools that only professionals have had into the hands of the public. God knows what will happen now."

Today, there are over 1.8 billion personal computers in use and that number is projected to reach 2 billion by 2015.[4] If the visionaries who conceived and developed the modern computer could not foresee the magnitude of how their ideas would become part of our daily lives and develop at an increasing speed, the idea that their invention would become the vehicle for an entirely new genre of crime was far beyond comprehension. Yet, while experts fretted about how the computer might result in social upheaval, the real social threat – cybercrime – was coalescing.

In this article, we examine the origins and current status of cybercrime, and identify the governing laws in the United States.

A brief introduction to cybercrime

In February 2009, 56 year-old Dave Crouse of Chicago, Illinois was surprised when a number of small but suspicious charges – $37 and $17.98 – appeared on his bank account. Six months later, $3,200 in unexplained debits was incurred in one day. He closed his accounts and opened new ones at a different bank. The very next day, his bank charged him $1,100. By February 2010,

[1] *The motto lives on today in the name of IBM's Thinkpad computers.*

[2] *It should be noted that computer historians debate whether Watson ever actually made this remark.*

[3] *Otto Friedrich, "Machine of the Year - The Computer Moves In" Time 3 January 1983, at http://www.time.com/time/magazine/article/0,9171,953632,00.html.*

[4] *Liz Webber, "Computer Use Expected to Top 2 Billion" Inc. Magazine, 2 July 2007, at http://www.inc.com/news/articles/200707/computers.html.*

nearly $1 million in merchandise, gambling, and telephone-services charges had been debited to his accounts or charged in his name. His attempts to salvage his finances have cost him nearly $100,000 and have reduced his savings and retirement accounts. In the middle of this nightmare, Dave lost his job in the construction industry. Soon he found that not only had hackers taken his money, they also cost him his livelihood. Although he holds a doctoral degree in organizational psychology and has a long history of contracting work at U.S. federal facilities, Mr Crouse failed to find a job. Finally, one recruiter explained that companies were rejecting him because his credit reports were so poor and his debt was mounting. Soon, his security clearance to work on government buildings was terminated. When he asked how this could have happened, the bank told him that malicious software was probably the cause of the problem. Mr Crouse was an avid on-line shopper, banked on-line, frequented eBay, purchased music on-line, and used his ATM card like a credit card. Unfortunately for Mr Crouse, somewhere in his on-line travels, his computer had become infected with a keystroke logger. The program picked up all his personal information by tracking every key he struck and transmitted it somewhere in the world to the program's author. Dave Crouse's life has been decimated by cybercrime. And he is not the only one. In 2009, one in every twenty Americans was the victim of some form of misappropriation of identity (commonly known as identity theft) – a new record – according to a recent study by Javelin Strategy and Research. That figure is up 12 per cent over 2008 and is 37 per cent ahead of 2007. "The odds have never been higher for becoming a fraud victim," said James Van Dyke, Javelin president and founder. "It's an easy crime to perpetrate, a crime that's almost impossible to catch when done in a sophisticated manner and a crime in which enforcement is very limited."[5]

Despite the increasing and nearly universal danger, cybercrime remains a threat that most people know little about. The purpose of this article is to provide an introduction to cybercrime from the perspective of the United States of America. Four areas will serve as the focus of the analysis: first, a historical and statistical look at the origins and current state of cybercrime; second, an examination of U.S. laws critical to the prosecution of cybercrime in America; third, the identification and discussion of unique problems posed to the investigation and prosecution of cybercrime as illustrated by selected case law, and finally, we will conclude by briefly exploring the special challenge of the judiciary in presiding over cybercrime prosecutions and enforcing cybercrime laws.

The origins and current state of cybercrime

Hackers and the origins of cybercrime

The first "hackers" emerged in the 1960s at M.I.T. and were more interested in toy trains than computers. They were members of a model train enthusiast group on campus who modified and rerouted toy train tracks and switches to make them perform faster and differently.[6] The term "hack" meant an elegant, witty or inspired way of getting things done.[7] M.I.T. students being M.I.T. students, it was not long before some of these train hackers began employing their rigging skills to the new mainframe computing systems being studied and developed on campus. The computer hacker was born. Inevitably, inspiration turned to exploitation. The first instance of network hacking occurred in 1972 when a man named John Draper discovered that a toy whistle given away inside Cap'n Crunch cereal generated a tone at 2600 MHz. This was the same frequency that enabled a person to obtain access to AT&T's long-distance switching system. Mr Draper, who became known by the moniker 'Cap'n Crunch', built a device he called a "blue box" that used the tone to make free telephone calls. Telephone hackers became known as "phreakers" and included Steve Wozniak and Steve Jobs, future founders of Apple Computer, who launched a home industry making and selling blue boxes.[8]

The internet

As clever as Cap'n Crunch and his contemporaries certainly were, their skills would have been of limited applicability without a means of obtaining access to their targets. A new Ferrari, beautiful as it may be, would be useless without a road upon which to travel. Fortunately for these hackers, the internet was already in the process of becoming both viable and accessible. If the computer was the vehicle of the cyber criminal, the internet was about to become the highway.

The internet was conceived as a child of the space

[5] *The facts outlined are taken from Jennifer Waters, "Identity fraud nightmare: One man's story," MarketWatch 10 February 2010 at http://www.marketwatch.com/story/the-rise-of-identity-theft-one-mans-nightmare-2010-02-10.*

[6] *PCWorld.com Staff, "Timeline: A 40-year history of hacking" CNN.com/SCI-TECH, 19 November 2001, at http://archives.cnn.com/2001/TECH/internet/11/19/hack.history.idg/*

[7] *Mark Ward, "Hacking: A history" BBC News Online, 27 October 2000, at http://news.bbc.co.uk/2/hi/science/nature/994700.stm.*

[8] *PCWorld.com Staff, "Timeline: A 40-year history of hacking".*

race in the late 1950s. On October 4, 1957 the Soviet Union launched the Sputnik satellite into orbit. Upon realizing that the Russians were in space and had developed the capacity to rapidly exploit military technology, the United States quickly passed legislation to address the nation's perceived technological shortcomings. Among the entities thereby created were the National Aeronautics and Space Administration (NASA) and the Advanced Research Projects Agency (ARPA). Four months later, NASA put a U.S. satellite into orbit. Nine months later, on December 18, 1958, the first communications satellite was launched and relayed a Christmas message from President Dwight D. Eisenhower to the world. America's space program was not all one-upsmanship and season's greetings, however – U.S. satellites were soon employed to create a network that enabled all elements of the military and government to maintain communications with one another under all circumstances.

Unprecedented as the U.S.'s new satellite network may have been, the technology was still very basic, and then, as now, was not without its flaws. Chief among them was that computers could only communicate to a single other computer to which it was directly linked. This lack of interconnectivity defined the problem that ARPA researchers worked for the next ten years to solve. Finally, in 1969, ARPA linked four host computers located at UCLA, the University of Utah, Stanford, and UC Santa Barbara. This network was called the ARPANet. By the spring of 1970, the ARPANet was linked to the east coast. In 1973, the network was linked by satellite to Hawaii and Norway. ARPANet continued to increase at the rate of one host every 23 days through the early 1980s. In 1982, the advent of the internet protocol allowed different networks to connect to each other. The foundation of the internet as we know it today had been laid.[9]

By the early 1980s, hackers had taken notice of the fledgling internet, and were already using electronic bulletin boards to gossip, trade tips, and share stolen computer passwords and credit card numbers. Particularly brazen hackers and groups of hackers had taken to infiltrating defense and corporate computer systems. In 1983, a group known as the 414 gang broke into computers at the Los Alamos National Laboratory, a facility that helps to develop nuclear weapons.[10] While *Time* magazine might have missed the activities of hackers, it did not take long for the wave of sensitive network break-ins to catch the attention of the United States government. In 1984, Congress passed the Computer Fraud and Abuse Act (CFAA), making it a crime to break into government and financial institution computer systems.[11] Despite Congress' intentions, the CFAA could do little to stem the tide of computer crime. When the CFAA was passed, internet users numbered only a few thousand – mostly university researchers and government agencies. By 1995 there were 16 million people on the internet. It comes, then, as no surprise that the world saw a statistical explosion in cybercrime starting in the 1990s.

Today there are over 1.8 billion internet users.[12] As internet use has increased and technology has evolved, hackers have been presented not only with more targets but also with new, more lucrative, opportunities. According to a 2009 survey by Javelin Research, 47 per cent of households in the United States – over 70 million[13] people – now do their banking on-line.[14] Another 22 million,[15] or 50 per cent,[16] do the same in the UK. Likewise, Craigslist has over 50 million users;[17] PayPal has over 78 million active accounts,[18] and eBay stopped counting after reaching 125 million users.[19] The internet has mutated from its genesis as a hub for researchers and government agencies to share information, and turned into a bustling center of international commerce. Suffice it to say, cybercrime has not lagged behind.

Cybercrime today

Perhaps the most telling statistics are not those that demonstrate how many people are doing their business on-line or why, but rather how many are not and why they are not. Among those who choose not to do their banking on-line, 41 per cent of consumers in the U.S. and 38 per cent in the UK credited security concerns as their most important reason for not banking over the

[9] *"Internet History," Computer History Museum, 2006 Computer History Museum, 2006, at http://www.computerhistory.org/internet_history/.*

[10] *PCWorld.com Staff, "Timeline: A 40-year history of hacking".*

[11] *Congress perhaps still did not understand all the aspects of cybercrime: the original version of the CFAA excluded juveniles from its purview.*

[12] *"Internet Usage Statistics" Internet World Stats, 31 December 2009, at http://www.internetworldstats.com/stats.htm.*

[13] *Brian O' Connell, "Study: Do Customers Prefer Online Banks?" BankingMyWay.com, 2010, at http://www.bankingmyway.com/save/study-do-customers-prefer-online-banks (citing the 2009 study by Javelin Research).*

[14] *Lance Whitney, "Online banking is booming" cnet News, 16 June 2009, at http://news.cnet.com/8301-1001_3-10265409-92.html.*

[15] *"Half of UK net users bank online" Finextra.com, 12 January 2010, at http://www.finextra.com/news/fullstory.aspx?newsitemid=20938.*

[16] *Lance Whitney, "Online banking is booming".*

[17] *"Site Profile for Craigslist.org" Compete Site Analytics, 20 March 2010, at http://siteanalytics.compete.com/craigslist.org/.*

[18] *"About Us" Paypal, 15 April 2010, at https://www.paypal-media.com/aboutus.cfm.*

[19] *Mary Jayne McKay, "eBay's Bid For Success - Internet Auction Site Racking Up Big Gains" CBS 60 Minutes, 5 January 2005, at http://www.cbsnews.com/stories/2002/10/30/60II/main527542.shtml.*

internet.[20] These consumers are right to be cautious, because current laws in the U.S. identify at least thirty different types of cybercrime. Given the pervasiveness of the threat and the high level of risk posed to consumers and corporations around the world, perhaps it is a wonder that so many people link their finances to the internet.

Statistics: costs and losses from cybercrime

While the precise magnitude of the financial cost of cybercrime is unknown, recent studies provide at least a rough framework for analysis. In 2005, the U.S. Government Accountability Office (GAO) estimated the annual loss due to computer crime for U.S. organizations to be $67.5 billion.[21] A 2009 study conducted by Javelin Strategy and Research found that losses from on-line misappropriation of identity caused losses of $54 billion to U.S. consumers and businesses.[22] A 2009 study by McAfee found that data theft and breaches from cybercrime may have cost businesses as much as $1 trillion globally in lost intellectual property and expenditures for repairing the damage last year.[23] As high as these figures are, what is most troubling is that all reports indicate that cybercrime is increasing at an increasingly rapid pace. Incidents of misappropriation of identity rose 12 per cent from 2008 to 2009. According to the U.S. Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3), the loss, just from cases referred to the IC3, amounted to $559.7 million in 2009.[24] This figure is an increase of 212 per cent from 2008 ($264.6 million) and an increase of 667.8 per cent (from $83.9 million) in 2001. 336,655 complaints were submitted to IC3 in 2009, a 22.3 per cent increase from 275,284 in 2008, and a 62.7 per cent increase from 206,884 in 2007.[25] According to the 2008 Computer Security Institute (CSI) Annual Computer Crime and Security Survey, the average cost of computer financial fraud to businesses and institutions that suffer it is $500,000.[26] For its 2009 report, CSI compiled data from 443 U.S. based respondents across the public and private sectors. Not surprisingly, the survey results indicated that cybercrime remains on the rise: 64.3 per cent of respondents experienced infection by malicious software, compared to 50 per cent in 2008; 29.2 per cent experienced denial-of-service attacks, compared to 21 per cent in 2008; 17.3 per cent experienced password sniffing, compared to 9 per cent in 2008, and 13.5 per cent experienced web site defacement, compared to 6 per cent in 2008.[27]

This brief survey represents limited results from discrete surveys. Nevertheless the message is clear: cybercrime presents significant and increasing threat to consumers, businesses, financial institutions, and governments all over the world.

Criminology: Modern cybercrime and the cyber criminal

Current laws in the U.S. provide for at least 30 different types of substantive cybercrime, including Denial of Service Attacks; Substitution or Redirection of a web site; Use of a Misleading Domain Name; Extortion; Internet Fraud (e.g. auction fraud or "phishing"); Credit Card Fraud; Sale of Prescription Drugs and Controlled Substances; Sale of Firearms; Gambling; Sale of Alcohol; Securities Fraud; Piracy and Intellectual Property Theft; Trade Secrets/Economic Espionage; Electronic Threats; Electronic Harassment; Interception of Electronic Communications; Cyber stalking; Espionage; Hate Crimes; Libel/Slander; Posting Personal Information on a Website (e.g., telephone numbers and addresses); Invasion of Privacy; Disclosure of Private Information; Spam; and Spoofing Email Addresses.

The culmination of many of these subsets of cybercrime, particularly those related to fraud and misappropriation of identity, is a new underground industry known as "carding." According to the U.S. Secret Service, "[c]ybercrime has evolved significantly, from dumpster diving and credit card skimming to full-

[20] *Gartner Press release "Gartner Survey Shows Number of Consumers in the U.S. and U.K. Using Online Banking Continues to Grow Across Income and Ages", June 15, 2009, at http://www.gartner.com/it/page.jsp?id=1020212 in respect of the Gartner report "Gartner Consumer Survey Shows That Barriers to Online Banking Use Continue to Fall".*

[21] *"Report to Congressional Requesters - CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats" U.S. Government Accountability Office (U.S. GAO, 70-705 June 2007), at http://www.gao.gov/new.items/d07705.pdf.*

[22] *Jennifer Waters, "Identity fraud nightmare: One man's story," MarketWatch 10 February 2010.*

[23] *Elinor Mills, "Study: Cybercrime cost firms $1 trillion globally," cnet News, 28 January 2009, at http://news.cnet.com/8301-1009_3-10152246-83.html.*

[24] *United States Federal Bureau of Investigation Internet Crime Complaint Center (IC3) "2009 Internet Crime Report" National White Collar Crime Center (NW3C), at http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf.*

[25] *2009 Internet Crime Report" National White Collar Crime Center (NW3C): This total includes many different complaint types, including both fraudulent and non-fraudulent crimes. Yet, research indicates that only one in seven incidents of fraud ever make their way to the attention of enforcement or regulatory agencies.*

[26] *Robert Richardson, "2008 CSI Computer Crime & Security Survey" Computer Security Institute, at http://www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf.*

[27] *Hilton Collins, "CSI Computer Crime and Security Survey Shows Poor Security Awareness Training in Public and Private Sectors," Computer Crime Research Center, 12 January 2010 at http://www.crime-research.org/news/12.01.2010/3758/.*

fledged online bazaars full of stolen personal and financial information."[28] In contrast to other types of misappropriation of identity, carding involves the large-scale theft of credit card account numbers and other financial information. As opposed to phishing and other means of misappropriation of identity, where the number of victims rarely exceeds several hundred, or in rare cases, a few thousand, carding is a global enterprise that often involves thousands of victims, and in some cases, millions.

A portrait of a new criminal activity

A man by the name of Max Butler serves to illustrate the development of the carding "profession". Butler began his hacking career as a teenager in Idaho, dabbling in telephone phreaking and reading hacker magazines in class. After his parents divorced in 1984, Butler found a new home on the internet and found a community on hacker message boards. Intelligent but socially awkward, Butler struggled with bullies through high school. In 1990, his first girlfriend broke up with him and he responded by putting his hands around her throat and threatening to kill her. In 1991, he was sentenced to five years in prison for the incident.[29] After his release from prison in 1995, Butler put his hacking skills to legitimate use. He earned a good living working as a network security auditor for corporate clients as well as the FBI. Butler's life as a white hat[30] would be short-lived, however. In 1998, Butler took it upon himself to hack into several government and military networks and fix a network security hole. In the process of doing so, however, Butler installed a small backdoor, securing for himself personal access to military bases, nuclear laboratories, and the U.S. Departments of Commerce, Transportation, and the Interior as well as the National Institute of Health. He was soon back in jail: in May 2001 he was sentenced to eighteen months in Taft federal prison. As the report by Poulsen indicates, it was this period in prison that would change the nature of Butler's hacking. Previously, Butler had hacked for the challenge and the personal accomplishment of breaking into supposedly secure systems. Butler was about to begin his transformation from trespasser to thief.

In prison, Butler met another hacker by the name of Jeff Normington, serving a sentence for wire fraud. After they were both released in 2002, Normington introduced Butler to Christopher Aragon, a man with capital and access to the criminal underworld. Aragon and Butler would rent rooms at hotels in San Francisco and use the antenna to locate the nearest high speed network. From there, Butler would launch his attacks, initially by stealing from other thieves. The stolen identity information, PINs, passwords, and credit card data was used to create false credit cards and go shopping for luxury items that the two could easily dispose of. He then began to hack into the systems of regional banks and steal fresh credit card information. He sold these to Aragon for upwards of $10,000 a month. Aragon set up an office to coordinate the operation: an assistant to help him with card printing and programming, and attractive young women who used the cards to buy expensive designer merchandise for resale on eBay.

Butler later expanded his 'business' by creating a carding site called CardersMarket.com. Within a year, CardersMarket had 1,500 buyers and sellers dealing in goods that ranged from simple stolen credit card numbers to packages that provided entire stolen identities including credit card and bank account information, PINs, counterfeit passports, drivers licenses, and Social Security Cards, birth certificates, college student identity cards, health insurance cards, and other false identification documents.[31] Butler later hacked into his four remaining competitors, transferred all their members to CardersMarket and then deleted their databases. Federal law enforcement officers took action when it was discovered that an attack against Capital One Bank was linked to a web site registered from the same account as CardersMarket. Although operating under an his alias, "Iceman", nevertheless traditional police investigations led them to Christopher Aragon, and a search of his house revealed incriminating evidence that led them directly to Butler. While the Secret Service watched Butler's residence, the FBI obtained a secret court order that allowed agents to monitor the IP addresses of visitors to CardersMarket. The FBI soon realized that it was no coincidence that several addresses were traced back to broadband

[28] *"Press Release: United States Secret Service's Operation Rolling Stone Nets Multiple Arrests," United States Secret Service, U.S. Department of Homeland Security, Washington: GPO, March 28, 2006, at http://www.justice.gov/criminal/cybercrime/ccnews.html.*

[29] *The facts relating to this case are largely taken from Kevin Poulsen, "Catch Me If You Can," Wired Magazine, January 2009, pp 95-126 and the authors wish to acknowledge credit to Mr Poulsen's article. For the ease of the reader, references have not been repeated; the article is also available on-line at http://www.wired.com/images/press/pdf/maxbutler.pdf.*

[30] *The term "white hat" refers to an ethical hacker or penetration tester who focuses on securing and protecting IT systems.*

[31] *Kimberly Kiefer Peretti, "Data Breaches: What the Underground World of "Carding" Reveals," Santa Clara Computer and High Technology Journal, Volume 25 number 2 (2008), pp 375-413, available on-line at http://www.chtlj.org/volumes/v25#v025.i2.Peretti.pdf.*

subscribers living within a block of Butler's apartment – the neighbours from whom Butler was stealing Wi-Fi. After he was arrested, the FBI found a million credit card numbers on his hard drive. In total, Butler stole nearly 2 million credit card numbers from banks, businesses and other hackers, which were used to obtain over $86 million in fraudulent charges.[32] Under the recently revised U.S. Sentencing Commission rules, it was the equivalent of a $500 million bank robbery. Butler was potentially looking at the first life sentence for hacking. Max Butler changed his name to Max Ray Vision while in prison. On February 12, 2010 Max Ray Vision was sentenced to thirteen years in prison and was required to pay $27.5 million in restitution. Despite being far less than the maximum, at the time it was the largest-ever prison sentence for a hacker.[33]

What may be most troublesome about this story is that Vision's enterprise can almost be considered to be innocuous when compared to some of his contemporaries.

Carding and misappropriation of identity have been linked to the funding of meth addiction and narcotics trafficking.[34] Arguably even more alarming is that the relationship between misappropriation of identity and the funding of terrorism is well established.[35] A convicted terrorist in Indonesia, Imam Samudra, specifically referred to the use of carding as a means of funding terrorist activities. Samudra sought to fund the 2002 Bali nightclub bombings through credit card fraud. In another case, three men used stolen credit card numbers to fund jihadist web sites. The men were members of one or more carding organizations of a similar nature to CardersMarket.[36]

The Max Butler story and the cybercrime statistics that precede it in this article may give rise to any number of inferences. However, what is demonstrated most clearly is the indisputable need for effective practical and legal mechanisms for responding to this growing threat. The next part of this article will explore those mechanisms.

Cybercrime laws in the United States

Thirty years ago, law enforcement agencies faced the emerging threat of cybercrime without the aid of any criminal statutes designed to deal with it. Wire fraud and mail fraud laws were employed where possible, but were often a poor fit for the conduct at issue.[37] However, as early as 1983, the U.S. government began to recognize the need for legislation that specifically addressed computer crime. Beginning with 18 U.S.C. § 1030 of the Comprehensive Crime Control Act of 1984,[38] the United States has vigilantly responded to this evolving menace by regularly enacting new laws and amending old ones as they become deficient. This section will explore cybercrime laws in the U.S. by focusing on three areas: the Computer Fraud and Abuse Act (CFAA) of 1986; other laws particularly relevant to specific types of cybercrime; and future legislation which may aid in dealing with such crimes.

The Computer Fraud and Abuse Act of 1986

Origins, purpose, and evolution

Faced with a wave of crimes not previously conceived, Congress intended to provide law enforcement, prosecutors, and computer users with "a clearer statement of proscribed activity".[39] Rather than amend criminal laws to account for computer-related offenses, Congress opted to address the issue in a single, new statute, 18 U.S.C. § 1030.[40] While 18 U.S.C. § 1030 was a step in the right direction, it quickly became evident that a more robust solution was necessary. Congressional hearings on the matter culminated in 1986 with the passing of the Computer Fraud and Abuse Act (CFAA), which is the main item of federal legislation dealing with computer crime.[41] The initial purpose of the CFAA was to protect classified information, financial records, and credit information on government and financial institution computers. To that end, the Act amended 18 U.S.C. § 1030 in a number of ways. It added additional penalties for fraud and related activities in connection with access devices and computers, as well

[32] *Kevin Poulsen, "Superhacker Max Butler Pleads Guilty," Wired Magazine 29 June 2009, http://www.wired.com/threatlevel/2009/06/butler_court/.*

[33] *That number has since been eclipsed. In March 2010, Albert Gonzales was sentenced to 20 years in prison for leading a group of cybercriminals that stole tens of millions of credit and debit card numbers from several U.S. retailers.*

[34] *Kimberly Kiefer Peretti, "Data Breaches: What the Underground World of "Carding" Reveals," at pp 391-92.*

[35] *Kimberly Kiefer Peretti, "Data Breaches: What the Underground World of "Carding" Reveals," at pp 391-92.*

[36] *Kimberly Kiefer Peretti, "Data Breaches: What the Underground World of "Carding" Reveals," at pp 391-92.*

[37] *Wire fraud and mail fraud statutes have not been abandoned in dealing with computer crime. Having since been amended to encompass computer-specific offenses, they are now regularly charged in conjunction with cybercrime-specific statutes and often carry stiffer penalties. For example, see, 18 U.S.C. § 1343.*

[38] *The CFAA amended 18 U.S.C. § 1030 of the Comprehensive Crime Control Act of 1984*

[39] *Scott Eltringham, "Prosecuting Computer Crimes" (United States Department of Justice - Computer Crime & Intellectual Property Section, February 2007), at http://www.justice.gov/criminal/cybercrime/ccmanual/index.html.*

[40] *Scott Eltringham, "Prosecuting Computer Crimes"*

[41] *The CFAA amended 18 U.S.C. § 1030.*

as additional protection for federal computers. It also criminalized additional computer-related acts and included provisions to penalize the theft of property via computer that occurs as a part of a scheme to defraud; to penalize those who intentionally alter, damage, or destroy data belonging to others, and to criminalize trafficking in passwords and similar items.

The Act was far more comprehensive than its predecessor, but it was not without limitations. Jurisdiction extended only to cases with "compelling federal interest," a phrase requiring either harm to computers of the federal government or certain financial institutions, or an effect on interstate commerce. Today, the prevalence of the internet has rendered nearly all computer use interstate in nature. At the time the CFAA was originally enacted, however, this jurisdictional language was far more limiting. Furthermore, despite the fact that minors committed many of the higher-profile computer crimes that had prompted the legislation, the CFAA excluded minors from its purview. Over the course of the last quarter-century, these deficiencies have been remedied. The Act has been amended eight times: in 1988, 1989, 1990, 1994, 1996,[42] 2001, by the USA Patriot Act 2002, and 2008 by the Identity Theft Enforcement and Restitution Act. The 1994 amendments added a civil cause of action for victims of cybercrime,[43] while the Patriot Act amendments[44] of 2001 made clear that "protected computers" includes computers outside of the U.S. providing they affect "interstate or foreign commerce or communications of the United States".[45]

Scope and applicability: Insider/Outsider

A dichotomy that pervades the CFAA is that of the insider versus the outsider. The different provisions of the CFAA apply differently – or may not apply at all – depending on whether the perpetrator is an insider who exceeds his authorization to protected computers or is an outsider who possesses no authorization at all. Traditional insider/outsider cases include *U.S. v. Czubinski*, 106 F.3d 1096 (1st Cir. 1997) and *U.S. v Ivanov*, 175 F.Supp.2d 367 (D.Conn.2001). In *Czubinski*, an Internal Revenue Service employee was found to have exceeded his authorized access to IRS computer systems when he looked at taxpayer records for personal purposes. Conversely in *Ivanov*, a Russian intruder broke into an American company's customer database and was found to have acted without authorization. This analysis applies to 18 U.S.C. §§ 1030(a)(1), (a)(2), (a)(3), (a)(4), (a)(5)(A)(ii), and (a)(5)(A)(iii), discussed below.

The CFAA includes provisions where authorization is not an element, including Damaging Without Authorization,[46] Trafficking in Passwords,[47] and Extortion Involving Threats to Damage a Computer.[48] The Act contains seven criminal provisions which prohibit the following acts: Obtaining National Security Information; Compromising Confidentiality; Trespassing in a Government Computer; Accessing to Defraud and Obtain Value; Damaging a Computer or Information; Trafficking in Passwords; and Threatening to Damage a Computer.

Laws particularly relevant to specific threats

Robust as the CFAA may be, its focus is often on crime in the form of unauthorized access to computers and systems. Accordingly, its scope is limited to crime at the physical and temporal point of access to protected systems – hacking. However, as computers have become increasingly user-friendly, so too has cybercrime. No longer does cybercrime necessitate actual "hacking" by itself. Moreover, even those crimes that do involve hacking often involve subsequent low-tech components, which escape the purview of the CFAA. To that end, the U.S. has promulgated laws to address these acts.

Identity Theft, Phishing, and Carding

The Identity Theft and Assumption Deterrence Act of 1998

Section 1028(a)(7) of the Identity Theft and Assumption Deterrence Act of 1998 18 U.S.C. § 1028 (ITAD) applies to network crimes, and prohibits a person from transferring, possessing, or using any means of identification of another person without authorization with the intent to engage in any activity that violates Federal law. The Identity Theft Penalty Enhancement Act of 2004 amended ITAD and added the offense of aggravated identity theft.[49] This scaled-up version adds an additional two-year term of imprisonment for identity

[42] *The National Information Infrastructure Protection Act of 1996 broadened the scope of protection offered by the Computer Fraud and Abuse Law by covering all computers attached to the internet and, therefore all computers used in interstate commerce. It also criminalized all unauthorized access of computer files in order to transmit classified government information; intentional access of U.S. department or agency non-public computers without permission; and accessing protected computers, without or beyond authorization, to defraud and obtain something of value.*

[43] *18 U.S.C. § 1030(g).*

[44] *18 U.S.C. § 1030(e)(2)(B).*

[45] *See also U.S. v. Ivanov, 175, F.Supp.2d 367 (D.Conn. 2001) (Congress intended the provisions of the CFAA to apply extraterritorially to computers used either in interstate or in foreign commerce).*

[46] *18 U.S.C. § 1030(a)(5)(A)(i).*

[47] *18 U.S.C. § 1030(a)(6).*

[48] *18 U.S.C. § 1030(a)(7).*

[49] *18 U.S.C. § 1028A.*

theft in connection with particular federal violations.

Access Device Fraud

Often charged alongside section 1028, section 1029 of the Access Device Fraud Act 18 U.S.C. §1029 prohibits the fraudulent use of "access devices" to steal money. "Access device" is defined broadly as "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or any other telecommunication service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)."[50] Charges under section 1029 are useful in many types of phishing cases, where a defendant uses fraudulent e-mails to obtain various types of passwords and account numbers, and carding cases where a defendant purchases, sells, or transfers stolen bank account, credit card, or debit card information. Conspiracy,[51] wire fraud,[52] and bank fraud[53] statutes may also be applicable in prosecuting these cases.

Spam

CAN-SPAM Act of 2003

The reader may recall from the introduction to this article, that inaccurate forecasts are common. The computer industry leaders of today are no different from their predecessors. In 2004, at the World Economic Forum, Bill Gates proclaimed that, "Two years from now, spam[54] will be solved."[55] Six years later, computer users the world over still await that solution. In an effort to control this problem, Congress passed the Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act of 2003 18 U.S.C. § 1037. Effective as of January 1, 2004, the Act sets the rules for commercial e-mail. It establishes requirements for commercial messages, bans false or misleading e-mail header information, and prohibits deceptive subject lines, gives recipients the right to be removed from mailing lists, and provides tough penalties for violations.[56] Although civil and regulatory provisions are the primary mechanism by which CAN-SPAM is enforced, the act also contains both misdemeanor and felony criminal provisions for particularly egregious offenses.[57]

It will not surprise the reader that the CAN-SPAM has not been totally successful. The reasons for its failure are several. First, and perhaps most importantly, the Act is not enforced.[58] In its first four years, the Federal Trade Commission brought only thirty actions against spammers.[59] This is particularly frustrating in light of strong evidence that more rigid enforcement could make drastic and immediate reductions in the volume of in spam.[60] Second, the sophistication of spammer techniques has outpaced efforts to counter them.[61] Third, in striking a necessary balance between private and public enforcement (and thereby avoiding a tidal wave of plaintiffs) Congress did not include a private right of action for consumers.[62] It is also fairly difficult for internet service providers (ISPs) to gain the standing necessary to initiate legal action.[63]

Other measures

The Electronic Communications Privacy Act of 1986 (ECPA), which amended the Wiretap Act, was intended by Congress to afford privacy protection to electronic communications.[64] Title I prohibits the interception of electronic communications, while Title II (also referred to as the Stored Communications Act) prohibits access to stored electronic information.[65] The EPCA contains exceptions for certain government or law enforcement

[50] *18 U.S.C. §1029(e)(1).*
[51] *18 U.S.C. § 371.*
[52] *18 U.S.C. § 1343.*
[53] *18 U.S.C. § 1344.*
[54] *Unsolicited commercial e-mail.*
[55] *Martin Lee, "Six years later, CAN-SPAM Act leaves spam problem unresolved" SC Magazine 16 February 2010, at http://www.scmaazineus.com/six-years-later-can-spam-act-leaves-spam-problem-unresolved/article/163857/.*
[56] *Vanessa J. Reid, "Recent Developments in Private Enforcement of the CAN-SPAM Act," at http://works.bepress.com/vanessa_reid/1; "The CAN-SPAM Act: A Compliance Guide for Business," FTC Bureau of Consumer Protection (Federal Trade Commission, September 2009), at http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm.*
[57] *Scott Eltringham, "Prosecuting Computer Crimes", p 87.*
[58] *Scott Bradner, "The CAN-SPAM Act as a warning," Security Central InfoWorld, 6 January 2009 at http://www.infoworld.com/d/security-central/can-spam-act-warning-613.*
[59] *Scott Bradner, "The CAN-SPAM Act as a warning," Security Central InfoWorld.*
[60] *Michael Osterman, "The spam problem was mostly solved last Tuesday" Network World, 18 November 2008, at http://www.networkworld.com/newsletters/gwm/2008/111708msg1.html.*
[61] *Chris Thompson, "A Snowshoe Winter: Our Discontent with CAN-SPAM," Spamhaus.org, 25 February 2009, at http://www.spamhaus.org/news.lasso?article=641; Martin Lee, "Six years later, CAN-SPAM Act leaves spam problem unresolved".*
[62] *Vanessa J. Reid, "Recent Developments in Private Enforcement of the CAN-SPAM Act".*
[63] *See Haselton v. Quicken Loans, Inc, (2010 WL 1180353, March 23, 2010) and Gordon v. Virtumundo, Inc., 575 F.3d 1040 (Court of Appeals, 9th Circuit 2009). For a short commentary, see Kevin Thompson, "Standing under the CAN-SPAM Act," Cyberlaw Central, 2 April 2010, at http://www.cyberlawcentral.com/2010/04/02/standing-under-the-can-spam-act/.*
[64] *18 U.S.C. §§ 2510-22 and 2701-12.*
[65] *Orin S. Kerr, "A User's Guide to the Stored Communications Act", 72 Geo. Wash. L. Rev. 1208 fn. 1 (2004) (discussing the distinction between Title I and Title II to ECPA).*

entities,[66] and for the entity providing the electronic communication service.[67]

In the Ninth Circuit, a violation of Title I of ECPA requires an interception simultaneous with its original transmission, rather than at some later point when the communication is stored. For example, in *Bunnell v. Motion Picture Ass' n of America*, 567 F.Supp.2d 1148 (C.D.Cal. 2007), the defendant hacked into the plaintiffs' e-mail system and reconfigured it so that every e-mail message would be copied and forwarded to his e-mail account. The court found that any communication acquired when in storage – even if that storage lasted only momentarily on the plaintiff's server – was not covered by the Wiretap Act. The *Bunnell* case cited an earlier case – *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002) – holding that a defendant who gained access to the plaintiff's secure web site and viewed items there did not violate the Wiretap Act.

Counsel dealing with stored communications should consult Title II of ECPA, the Stored Communications Act (SCA). Generally, the SCA prohibits providers of communication services from disclosing private communications to certain persons or entities.[68] The SCA has been held to protect e-mail messages stored on an ISP's servers even after the ISP delivered the messages and continued to store the messages for the purpose of back-up protection.[69]

Future legislation

On March 23, 2010, U.S. Senators Kirsten Gillibrand (D-NY) and Orrin Hatch (R-UT) introduced a bill entitled the International Cybercrime Reporting and Cooperation Act.[70] The legislation seeks to deal with the ability of cyber criminals to operate with impunity across international borders, and would introduce new protocols for addressing the problem.[71] The bill would require the President to annually assess and report to Congress on the state of other nations' use of information and communications technologies (ICT) in critical infrastructure, the extent and nature of cybercrime based in each country, the adequacy and effectiveness of each country's legal and law enforcement systems addressing cybercrime, and countries' protection of consumers and commerce on-line. The President would also report on multilateral efforts to prevent and investigate cybercrime, including U.S. actions to promote such multilateral efforts. Thereafter, the bill would require the U.S. to develop programs for countries with low ICT penetration to prevent cybercrime and develop action plans for countries identified as cyber concern.

Evidentiary challenges

Yet another unexpected consequence of the computer revolution has been the digitalization of evidence. The major form of evidence is now *digital*.[72] Yet as pervasive as digital evidence may now be, it remains complicated for investigators to find and preserve, and difficult for lawyers and judges to adequately address in a court. It is imperative that cybercrime investigators be familiar with the technology underlying a cybercrime case, a point noted by Sgt. Ronald Levine of the Foothill-DeAnza College District Police Department in Los Altos Hills, California, in words that are probably echoed by every authority investigating cybercrimes across the globe: "If an officer or deputy doesn't have computer skills, they're going to have to come up to speed and understand how the technology works before he or she can become an effective investigator."[73] To that end, the U.S. Department of Justice has published *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*,[74] which sets out important guidelines for investigators to follow when investigating computer crimes and serves as a valuable digital evidentiary rubric for both prosecutors and defense counsel.

Foundational issues

Digital evidence must be authenticated to be admissible into evidence.[75] That is, it must be shown to be what the proponent claims it is. Because of the ease with which such evidence can be modified, authentication of digital evidence is an even more critical and difficult task than authentication of more traditional forms of tangible

[66] *18 U.S.C. § 2701(c)(3).*

[67] *18 U.S.C. § 2701(c)(1); BI3 v. Hamor, 2009 WL 2192801 (N.D.Ill. July 15, 2009) (holding that the statute did not protect against the interception of messages on a web site by that web site's network director).*

[68] *Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 900 (9th Cir. 2008).*

[69] *Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).*

[70] *The reference to this appears on the web sites of both Senators.*

[71] *Robert McMillan, "Proposed US law would single out cybercrime havens," Reuters, IDG News Service\San Francisco Bureau, 23 March 2010, at http://www.reuters.com/article/idUS190003768320100324.*

[72] *Stephen Mason, gen ed, International Electronic Evidence (London: British Institute of International and Comparative Law, 2008), p xxxviii.*

[73] *David Griffith, "How To Investigate Cybercrime" Police Magazine, 1 November 2003, at http://www.policemag.com/Channel/Technology/Articles/2003/11/How-to-Investigate-Cybercrime.aspx; this is starkly illustrated in the case of State of Connecticut v. Julie Amero, (Docket number CR-04-93292; Superior Court, New London Judicial District at Norwich, GA 21; 3, 4 and 5 January 2007). For a detailed analysis of this case, see Stephen Mason, gen ed, International Electronic Evidence (2008) pp xxxvi-lxxv.*

[74] *Available on-line at http://www.ncjrs.gov/pdffiles1/nij/199408.pdf*

[75] *Federal Rule of Evidence 901(a).*

evidence. However, the task is made somewhat less daunting by the permissive authentication standard utilized in the U.S. Federal Rules of Evidence. The proponent of the evidence need only make a *prima facie* showing of authenticity "so that a reasonable juror could find in favor of authenticity or identification."[76] Once the proponent clears this low hurdle, the probative force of the evidence is an issue for the jury. At this point, any doubts as to the authenticity of the evidence go to its weight and not its admissibility.

The difference between computer-stored and computer-generated evidence

Questions of authenticity often require making a distinction between *computer-stored* evidence and *computer-generated* evidence.[77] Computer-stored evidence includes documents that were created by a human being and that just happen to be stored in electronic form.[78] Examples include word-processing files, e-mails, and internet chat room messages. Computer-generated evidence, on the other hand, consists of the direct output of computer programs.[79] Examples include the login record of an ISP, automated telephone call records, and automatic teller receipts. Finally, some evidence may combine both forms. For example, a financial spreadsheet contains both the input data provided by a person and the output of a computer program.[80]

Authentication of computer-stored evidence

To authenticate computer-stored evidence, the proponent must identify the author of the record and show that it has not undergone any significant changes.[81] Both of these points can be shown through chain-of-custody testimony and other circumstantial evidence. Federal Rule of Evidence 901(b)(1) provides for authentication through "testimony of a witness with knowledge" that "a matter is what it is claimed to be."

For example, the prosecution in a criminal drug case may want to authenticate records of illegal drug transactions found in a computer seized from the defendant. The prosecution's authentication witness does not have to show how the computer was programmed or how the records were actually entered into the computer. Instead, the prosecution must establish two main points: the computer was found in the defendant's possession and the names used match those associated through other evidence with the drug transaction, and that the records are actually those found on that computer.[82] The former can usually be established by the officer investigating the case, while the latter can be established by a digital evidence specialist who examined the computer.

However, courts will exclude evidence when unsatisfied with explanations of the digital record-keeping system. In *In re Vee Vinhnee*, 336 B.R. 437, 448-49 (9th Cir. 2005), the court excluded American Express credit card billing statements because "[t]here is no information regarding American Express' computer policy and system control procedures, including control of access to the pertinent databases, control of access to the pertinent programs, recording and logging of changes to the data, backup practices, and audit procedures utilized to assure the continuing integrity of the records." The proponent of such evidence needs to take care to persuade the court that the digital records are securely maintained and not subject to alteration.[83]

Authentication becomes more difficult when the proponent claims that a certain person wrote it. For example, consider how to introduce into evidence a transcript of an internet chat-room conversation between two men, one of whom the prosecution alleges was the defendant. Using on-line aliases, the two men did not reveal their true identities on the transcript, so authentication will depend on circumstantial evidence. Perhaps evidence seized from the defendant's residence confirms something he said in the chat room. Also, information obtained from the ISP may be sufficient to show authorship.[84]

E-mails

E-mails are a form of computer-stored evidence. They are generally offered as written print-outs from a computer rather than through bringing the actual electronic image into court. Authenticating the e-mail itself is a simple matter of having a witness testify that he or she has seen the original and that the print-out is an accurate reproduction. However, authentication

[76] *United States v. Blackwood, 878 F.2d 1200, 1202 (9th Cir. 1989).*

[77] *'Digital Evidence in the Courtroom: A Guide for Law Enforcement & Prosecutors' (National Institute of Justice, 2007) (hereinafter referred to as 'Digital Evidence'), available at http://www.ojp.usdoj.gov/nij/pubs-sum/211314.htm and Stephen Mason, gen ed, Electronic Evidence (2nd edn, LexisNexis Butterworths, 2010) 4.01.*

[78] *'Digital Evidence'.*

[79] *'Digital Evidence'.*

[80] *'Digital Evidence'.*

[81] *'Digital Evidence'.*

[82] *'Digital Evidence' at § 9:9 (West 2010).*

[83] *For further discussion of this case, see Stephen Mason, gen ed, Electronic Evidence, 4.44 – 4.12.*

[84] *'Digital Evidence'.*

becomes more difficult when a prosecutor is trying to link the e-mail to the defendant, and the defendant denies authorship. In this situation, other evidence must be used. Certainly testimony by a witness who saw the defendant write and send the e-mail communication would suffice. That is rare, however. More common are circumstances where the sending computer is owned by the defendant, seized from the defendant's possession, or linked to the defendant through other compelling facts. This may be enough to authenticate the e-mail as one sent by the defendant. However, if it is a computer to which others had access, a court may require additional evidence linking the defendant to the e-mail in question.[85] For example, if it can be shown that the defendant was the one using the computer at the time the message was sent, this should suffice.[86]

Prosecutors sometimes call technical witnesses who can trace the e-mail in question. "A technical witness may rely on the coded Internet Protocol Address appearing in the e-mail header and trace it back to the internet service provider who relayed the message and sometimes back to a particular computer."[87] The most common method of authenticating e-mails is under Fed. R. Evid. 901(b)(4), by showing "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." An example of this can be found in *U.S. v. Safavian*, 435 F. Supp.2d 36 (D.D.C. 2006). In that case, e-mails were authenticated by four distinctive characteristics: the actual e-mail address; the name of the person connected to that address; the names of the senders and receiver in the e-mail; and their content, which discussed matters relating to individuals in question.

By itself, the fact that a person's name appears in the header as the "sender" is not enough, because it is so easy to alter the header. In *Victaulic Co. v. Tieman*, 499 F.3d 227, 236 (3d Cir. 2007), the Third Circuit held that the trial court erred in taking judicial notice of facts about the plaintiff's company based on its web site, because anyone may purchase a web address. The Circuit pointed out that the presence of a trade name in the URL does not authenticate a web site, and held that judicial notice is permitted only from sources not subject to reasonable dispute. Stronger circumstantial evidence would be a showing that the actual e-mail address, e.g., mailto:johndoe@aol.com, matches an account in that person's name with the indicated internet service provider, although this is not necessarily sufficient by itself because it is not technically difficult to send an e-mail message using another's e-mail address.[88]

Courts have often relied on the content of the message as a basis for authenticating e-mails, for which see *U.S. v. Safavian*, 435 F.Supp. 36, 39-40 (D.D.C. 2006) where e-mails were authenticated in part by their content which discussed personal and professional matters relating to individuals in question. If an e-mail contains particular information that only the purported sender is likely to know, this will authenticate the e-mail to the same extent that such knowledge would authenticate a written message.[89] Obviously the more specialized or unique the information, the more such content tends to authenticate the message as being from a particular sender who has such knowledge.[90] A reply e-mail can often be used for authentication purposes. "An e-mail purporting to be a reply to an earlier message sent to a particular person is likely to be authored by that person."[91] Often an e-mail message will include the message to which it is responding as an attachment or even in the body of the message. Even though it is possible that a reply is sent by a person other than the recipient of the original message, the danger is no greater here than for hand-written or typed messages.[92]

Authentication of computer-generated evidence

The authentication of computer-generated evidence is governed by Federal Rule of Evidence 901(b)(9) which provides for authentication by "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result." Authentication under Fed. R. Evid. 901(b)(9) can generally be accomplished by evidence that: (1) the computer equipment is accepted in the field as standard and competent and was in good working order;[93] (2) qualified computer operators were employed; (3) proper procedures were followed in connection with the input and output of information; (4) a reliable software

[85] '*Digital Evidence*'.
[86] '*Digital Evidence*'.
[87] '*Digital Evidence*'.
[88] *Federal Rule of Evidence 901(a) at § 9:9.*
[89] *As in the English case of R v Mawji (Rizwan) [2003] EWCA Crim 3067, [2003] All ER (D) 285 (Oct), 2003 WL 22477344 (CA (Crim Div)) discussed in Stephen Mason, gen ed, Electronic Evidence, 4.14.*
[90] *U.S. v. Siddiqui, 235 F.3d 1318, 1322, (11th Cir. 2000) (e-mails authenticated as written by defendant because they showed knowledge of actions only the defendant would be likely to be aware of, apologized for things the defendant himself had done, came from his e-mail address, and were signed with his distinctive nickname).*
[91] *Federal Rule of Evidence 901(a) at § 9:9.*
[92] *Federal Rule of Evidence 901(a) at § 9:9.*
[93] *Note the discussion of this topic in Stephen Mason, gen ed, Electronic Evidence, Chapter 5.*

program was utilized; (5) the equipment was programmed and operated correctly; and (6) the exhibit is properly identified as the output in question.[94]

Not all courts require each of these, however. The Ninth Circuit Court of Appeals has held that "[i]t is not necessary that the computer programmer testify in order to authenticate computer-generated records."[95] A computer print-out may be authenticated by "one who has knowledge of the particular record system."[96] Similarly, a party "need not produce expert testimony as to [the] mechanical accuracy of [a] computer where it presented evidence that [the] computer was sufficiently accurate [so that the] company relied upon it in conducting its business."[97] In the *U-Haul* case, an insurance manager testified about computer-generated summaries produced by his company. He testified regarding the process of inputting data into the computer and the process of querying the computer to compile the information to create the summaries. He testified that he was familiar with the record keeping practices of the company, and explained both the computer system used to compile and search the insurance claim records, and the process of querying the computer system to create the summaries that were admitted at trial. The court found this sufficient under Rule 901 to authenticate the summaries.[98]

Hearsay issues

Computer-stored evidence and hearsay

If the computer-stored evidence contains statements made by a person and is offered to prove the truth of the matter asserted, it is hearsay under Federal Rule of Evidence 801(c), unless it is offered against a party and is that party's own statement (Rule 801(d)(2)) or is a certain type of statement by a witness (Rule 801(d)(1). Under Rule 802, hearsay is not admissible unless it falls within the exceptions contained in Rule 803.

The most common hearsay exception for computer-stored records is the business records exception contained in Rule 803(6).[99] "It is immaterial that the business record is maintained in a computer rather than in company books."[100] To establish the foundation for this exception, the prosecution must show that: (1) the computer equipment (hardware and software) on which the record was stored is recognized as standard in the field or reliable;[101] (2) the data were entered by a person with knowledge in the regular course of business at or reasonably near the time of the occurrence of the event recorded; and (3) the sources on which the record was based, as well as the method and time of preparation indicate that the record is trustworthy and its admission is justified.[102]

While many attorneys practicing in the United States routinely argue that the business records exception covers any document which a company maintains in its files, the exception is actually much narrower than that. It is limited only to the data which the business entity routinely enters or maintains in its files or computers in the ordinary course of its operations. But even with this limitation, it is of great value to the litigator who is seeking to introduce computer-stored records from a business operation.

Computer-generated evidence and hearsay

The hearsay rule applies to "computer-generated evidence which repeats or contains human declarations. Evidence to which this hearsay rule may apply includes accounting records, invoices, summaries or any other types of computer output which reiterate human declarations which have been inputted into the computer."[103] The business record exception contained in Rule 803(6) applies not only to *computer-stored* evidence, as discussed above, but also to *computer-generated* evidence.[104] There are situations, however, where computer-generated evidence is not hearsay. For example, the issue may center on the computer key strokes themselves – that is, what the key strokes were, or, perhaps, when and at which terminal they were made. The human making the key strokes is not a declarant, because he is not making a statement about the transaction; he is performing the transaction itself.

[94] *Federal Rule of Evidence 901(a) at 9:20.*
[95] *U-Haul v. Lumbermens, 576 F.3d 1040 (9th Cir. 2009).*
[96] *U-Haul v. Lumbermens, 576 F.3d 1040 (9th Cir. 2009).*
[97] *U-Haul v. Lumbermens, 576 F.3d 1040 (9th Cir. 2009); although on this matter, note the comments by George L. Paul, Foundations of Digital Evidence (American Bar Association, 2008) p 129 and Stephen Mason, gen ed, Electronic Evidence, Chapter 5.*
[98] *U-Haul v. Lumbermens, 576 F.3d 1040 (9th Cir. 2009).*
[99] *'Digital Evidence', p 31.*
[100] *Sea-Land Service Inc. v. Lozen Intern. LLC, 285 F.3d 808 (9th Cir. 2002).*
[101] *Note the discussion of 'reliability' in Stephen Mason, gen ed, Electronic Evidence, Chapter 5.*
[102] *Sea-Land Service Inc. v. Lozen Intern. LLC, 285 F.3d 808 (9th Cir. 2002).*
[103] *Teneille Brown and Emily Murphy, 'Through a Scanner Darkly:Functional Neuroimaging as Evidence of Criminal Defendant's Mental States', 62(4) Stanford Law Review, 1119-1208 at fn 131 (April 2010).*
[104] *U-Haul v. Lumbermens, 576 F.3d 1040 (9th Cir. 2009) at 1043-45 (holding that computer data compiled in the ordinary course of business, summarized in computer-generated reports, and presented in computer print-outs prepared for trial is admissible under Rule 803(6)); see also B. Weinstein and M. A. Berger, Weinstein's Federal Evidence § 901.08[1] (2d. ed.2006) (stating that "print-outs prepared specifically for litigation from databases that were compiled in the ordinary course of business are admissible as business records to the same extent as if the print-outs were, themselves, prepared in the ordinary course of business. The important issue is whether the database, not the print-out from the database, was compiled in the ordinary course of business").*

If, then, a computer records the key strokes, processes them, and produces a print-out purporting to indicate what they were, such a print-out is not hearsay.[105] The admissibility of the print-out depends on authentication under Rule 901: If the computer hardware and software are electronically and mechanically sound, the print-out will be an accurate portrayal of the transaction; if they are unsound, it may not be.

Search and seizure

Digital evidence exists in many forms. The form sought by law enforcement agents will be critical to the legality of the seizure. For example, the agents may only want to seize a particular computer. That hard drive, however, may not contain what they are looking for; critical data may be stored on a network. Even stored data may be insufficient and additional information in the form of real-time traffic data – log-in times and dates, and ISP addresses collected from a service provider – might be critical to an investigation. Finally, law enforcement may want to seize not only the traffic data of digital messages, but also their content. Governing these searches and seizures are a variety of federal statues and the Fourth Amendment to the U.S. Constitution. If the search and seizure violates these authorities, the evidence that is seized may be excluded from evidence, although that is not always required. This section will discuss the governing authorities.

Wiretap Act

The Wiretap Act, 18 U.S.C. § 2510, governs the seizure of the content of digital messages. For example, police can install "sniffer" software that captures a hacker's instant messages.[106] The Wiretap Act prohibits anyone in the United States from intercepting the contents of wire, oral, or electronic communications. Violation of the Act can lead to criminal and civil penalties. For example, the Act was violated by a defendant who copied e-mail messages existing on a third-party provider's hard drive awaiting delivery to recipients.[107] The one exception is that interception may be authorized by an order of a court of competent jurisdiction. The Wiretap Act contains strict requirements for judicial approval. It requires advance approval by a federal judge, and is substantially stricter than the requirements for obtaining a warrant to search tangible property. Before issuing authorization under the Wiretap Act, the federal judge must find:

a) Probable cause to believe that an individual is committing, has committed, or will commit, one of a list of specified crimes;

b) Probable cause that the communications concerning the offense will be obtained through the interception;

c) That normal investigative techniques have been tried and failed, or are unlikely to succeed, or are too dangerous; and

d) Probable cause that the facilities from which the communications are to be intercepted are being used in connection with the commission of the crime.[108]

Interception becomes an integral part of the investigation after other investigative techniques fail.

Pen Register and Trap and Trace Statue

The seizure of real-time traffic data – dialing, routing, addressing, and signaling information provided by a communications service provider – is governed by the Pen Register and Trap & Trace Statute, 18 U.S.C. § 3121. This statute does not govern the seizure of content. A pen register records the outgoing connection information such as the telephone number dialed by a person under surveillance.[109] A Trap & Trace device records the incoming connection information such as the telephone number of the party who is calling the person under surveillance. The statute generally prohibits the nonconsensual real-time acquisition of non-content information by any person about a wire or electronic communication unless a statutory exception applies.[110] When no exception applies, law enforcement officers must obtain a pen/trap order from the court before acquiring noncontent information covered by the statute.[111] Note that the Ninth Circuit Court of Appeals has held that even if the pen register statute was violated, the statute does not require suppression of the evidence seized – providing it is merely traffic data and not content.[112]

[105] *'Digital Evidence', p 34.*
[106] *'Digital Evidence', p 34.*
[107] *U.S. v. Councilman, 418 F.3d 67 (1st Cir. 2005) (en banc).*
[108] *18 U.S.C. § 2518(3)(a)-(d).*
[109] *'Digital Evidence', p 2.*
[110] *'Digital Evidence', p 2.*
[111] *'Digital Evidence', p 2.*
[112] *U.S. v. Forrester, 512 F.3d 500 (9th Cir. 2008).*

Stored communications provisions of the Electronic Communications Privacy Act

The Stored Communications Act, 18 U.S.C. § 2701 (and following), protects individuals' privacy and proprietary interests. The Act protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility.[113] The Act applies when law enforcement officials seek to obtain records about a customer or subscriber from a communication service provider.[114] For example, the Act may apply when law enforcement seeks to obtain copies of a customer's e-mails from an internet service provider. Note that the act would not apply if the seizure of the e-mails was from the customer's own computer.[115] Under the Act, the production of some information may be compelled by subpoena, some by court order, and some by search warrant. The more sensitive the information, the higher the level of legal process required to compel disclosure.[116]

Fourth Amendment

The Fourth Amendment to the United States Constitution provides that: "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the person or things to be seized." In very general terms, the Fourth Amendment is construed as prohibiting the search or seizure of an individual or their property, unless a warrant is first obtained from a judge or the circumstances fall within a very limited number of situations where a warrant is deemed unnecessary – the "exceptions" to the search warrant requirement. This protection is extended to all activities and objects in which an individual has a reasonable expectation of privacy.

A warrant authorizing the search and seizure of computers or computer equipment must be supported by probable cause. It also must be sufficiently particular in its description of the digital evidence sought. A warrant violates the particularity requirement when, for example, it contains no restrictions on the search, no references to statutes, and no references to crimes or illegality.[117] Similarly, a warrant was found to be an over-broad "catch-all" warrant when it called for the seizure of all computers, all computer storage devices, and all computer software systems.[118] Finally, a warrant authorizing a search of the text files of a computer for documentary evidence pertaining to a specific crime will not authorize a search of image files containing evidence of other criminal activity.

Warrants for digital evidence in the Ninth Circuit

Given the cases just discussed, the government cannot just obtain a warrant to seize a computer and then rummage through it looking for evidence of a crime; rather, the government must specifically describe the evidence it seeks. But even when the warrant is specific, agents often must search through much unrelated material on the computer to find the specific material the warrant covers. Sometimes the unrelated material they view will be evidence of a crime. In such instances, the material is not covered by the warrant, and so the seizure of such material violates the Fourth Amendment unless an exception applies. Agents have claimed that the "plain view" doctrine applies – if evidence is in plain view, and is incriminating on its face, a warrant is not required.[119] If the courts accept the claim, law enforcement agents may have an incentive to seize more rather than less. One court described the issue this way: "Let's take everything back to the lab, have a good look around and see what we might stumble upon."[120]

Concerned about this perverse incentive, the Ninth Circuit Court of Appeals has imposed limitations on how the "plain view" doctrine applies in this setting. "To avoid this illogical result, the government should, in future warrant applications, forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data. If the government doesn't consent to such a waiver, the magistrate judge should order that the seizable and non-seizable data be separated by an independent third party under the supervision of the court, or deny the warrant altogether."[121]

Searches without a warrant

While the Fourth Amendment generally requires a warrant, there are exceptions for: (1) consensual

[113] *Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).*
[114] *'Digital Evidence', p 3*
[115] *'Digital Evidence', p 3*
[116] *'Digital Evidence', p 3*
[117] *U.S. v. Clough, 246 F.Supp.2d 84 (D. Me. 2003), on reconsideration in part, 255 F.Supp.2d 3 (D. Me. 2003).*
[118] *U.S. v. Hunter, 13 F.Supp.2d 574 (D. Vt. 1998).*
[119] *'Digital Evidence', p 10.*
[120] *U.S. v. Comprehensive Drug Testing, Inc, 579 F.3d 989, 998 (9th Cir. 2009).*
[121] *U.S. v. Comprehensive Drug Testing, Inc, 579 F.3d 989, 998 (9th Cir. 2009).*

searches, (2) exigent circumstances, (3) searches incident to arrest, (4) inventory searches, (5) and evidence seized under the plain view doctrine.[122] A voluntary consent will validate a warrantless search of a computer. Yet the scope of the search must not exceed the scope of the consent.[123] The government bears the burden of showing that the search did not exceed the scope of the consent.[124] If the law enforcement officials have a combination of probable cause and exigent circumstances, they can conduct a warrantless search of a residence.[125] The term "probable cause" requires that under the "totality of circumstances" known to the officers at the time they entered the residence, there was a "fair probability" that contraband or evidence of a crime would be found inside.[126] Exigency only exists in a few emergency situations such as the hot pursuit of a fleeing felon or a reasonable fear that without immediate seizure the evidence will be destroyed while a warrant is obtained.[127]

Traffic data and the Fourth Amendment

The United States Supreme Court has held that the use of a pen register to capture numbers dialed from a telephone line does not constitute a search for Fourth Amendment purposes.[128] According to the court, people do not have a reasonable expectation of privacy in the telephone numbers they dial because they "realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."[129] The Ninth Circuit Court of Appeals has extended this ruling to apply to the capture of digital traffic data such as the to and from addresses of e-mail messages, the IP addresses of web sites visited and the total amount of data transmitted to or from an account.[130] The Circuit reasoned that "e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the web sites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."[131] It was critical to the Circuit that no content was intercepted.

Conclusion: the role of the independent judiciary

As discussed, the threat of cybercrime is one that is both constantly increasing and evolving. One important aspect that is critical to mounting an adequate response to this threat is investigative and legal knowledge. The other critical element is that of an active and independent judiciary providing necessary oversight.

The tools of the cyber-criminal – technology and anonymity – have also become important assets in the range of responses of law enforcement. Moreover, much like traditional police work, many cybercrime investigations require investigators to go under-cover. Under federal law, warrants crucial to executing an effective investigation must be specifically approved in advance by a federal district judge or magistrate judge. Issues may arise in under-cover operations as to whether the law enforcement activities constituted entrapment or otherwise violated the rights of the accused. A federal judge will often be charged with making that difficult decision.

What is at issue, perhaps, is the role and attitude of the judiciary in dealing with cybercrime. At first blush, it may appear that the contents of this article may encourage an active role for the judiciary. Indeed, the challenges of investigating and prosecuting such activities would suggest the appropriateness or even the necessity of such an active role. However, whenever a federal judge begins to feel a bit of a kinship with the prosecutors who appear in their court, they should remind themselves of the words of Byron White, a former member of the U.S. Supreme Court, when he pronounced firmly that, "[j]udges and magistrates are not adjuncts to the law enforcement team; as neutral judicial officers, they have no stake in the outcome of particular criminal prosecutions."[132]

A truly independent judiciary is essential to the criminal justice system for at least three reasons.

First, it ensures that the rights of participants in our legal systems will not be abused. This has been the primary role of the federal judicial system from the founding of our country. Indeed, it was the abuse of search warrants which provided one of the precipitating

[122] *'Digital Evidence', pp 9-10.*
[123] *United States v. McWeeney, 454 F.3d 1030, 1034 (9th Cir. 2006).*
[124] *See generally United States v. Reid, 226 F.3d 1020, 1025 (9th Cir. 2000) (holding that government bears the burden of showing "the existence of effective consent").*
[125] *LaLonde v. County of Riverside, 204 F.3d 947 (9th Cir. 2000).*
[126] *Illinois v. Gates, 462 U.S. 213, 238 (1983).*
[127] *LaLonde v. County of Riverside, 204 F.3d at 956.*
[128] *Smith v. Maryland, 442 U.S. 735 (1979).*
[129] *Smith v. Maryland, 442 U.S. 735 (1979) at 742.*
[130] *U.S. v. Forrester, 512 F.3d 500 (9th Cir. 2008).*
[131] *U.S. v. Forrester, 512 F.3d 500 (9th Cir. 2008) at 510.*
[132] *United States v. Leon, 468 U.S. 897, 917 (1984).*

causes for our War of Independence. This role of the judiciary, as the bulwark which protects the rights of ordinary citizens, continues to be a hallmark of the American legal system.

Second, an independent magistrate overseeing criminal investigation will lead to great professionalism on the part of criminal investigators and prosecutors. This has come to be an accepted view among prosecutors and investigators in the United States. In recent years, the U.S. Supreme Court has had occasion to re-examine[133] one of the most significant precedent requiring judicial oversight of police investigative techniques – *Miranda v. Arizona* 384 U.S. 436 (1966). *Miranda* requires that a suspect's confession cannot be used against him at trial unless he was advised of his right to remain silent. In addition, conservative legal scholars have called for reversal of the 1961 decision of *Mapp v. Ohio*, 367 U.S. 643 (1961), which requires the exclusion of evidence obtained without a warrant in violation of the Fourth Amendment to the U.S. Constitution. When the *Miranda* and *Mapp* decisions were issued by the Supreme Court, there was a great deal of protest. The view was commonly expressed that they would reduce the effectiveness of the police in their efforts to deal with crime. However, despite conservative dissatisfaction, the Supreme Court, in a 7-2 decision, declined to reverse *Miranda*. And there has been a surprising lack of support in the law enforcement community for overturning either *Mapp* or *Miranda*. Perhaps that it is because the law enforcement community has come to realize that judicial oversight resulting from these decisions has led to increased professionalism in law enforcement, enhanced accuracy in the outcome of criminal investigations, and greater long-term success in dealing with crime.

Third, the independent judiciary offers legitimacy to the criminal justice system and our legal institutions. Although the United States judiciary takes pride in its commitment to the Rule of Law, it also recognizes that its commitment to that fundamental principle means very little if the public have serious reservations about the legitimacy, even-handedness, and fairness of our criminal justice systems. Knowledge that a truly independent judiciary provides real and meaningful oversight of criminal investigations creates greater respect for our legal system at all levels.

Thus, despite the need to ensure that critical personnel are proactive in acquiring the technological, investigative, and legal prowess required to ferret out and address cybercrime, it is critical that the judiciary maintain its independent role to prevent investigative abuses, improve the quality of law enforcement, and lend credibility to law enforcement activities.

The Honorable B. Lynn Winmill is the Chief Judge at the United States District Court for the District of Idaho.

David L. Metcalf is Staff Counsel in Judge Winmill's Chambers.

Michael E. Band was an Extern in Judge Winmill's Chambers, and is now an Associate with the firm of Davison, Copple, Copple & Copple.

[133] *For instance, see Dickerson v. United States, 530 U.S. 428 (2000).*

