INFORMATION BRIEF
Research Department
Minnesota House of Representatives
600 State Office Building
St. Paul, MN 55155

Ben Johnson, Legislative Analyst, 651-296-8957
Mary Mullen, Legislative Analyst, 651-296-9253
May 2018

The Internet and Public Policy: Criminal Activity on the Internet

This is one of a series on public policy and the Internet, with special attention to the laws and public policies of the state of Minnesota.

This publication discusses criminalization of Internet activities and provides information on federal and state laws enacted to address Internet-related crimes.

Contents

Copies of this publication may be obtained by calling 651-296-6753. This document can be made available in alternative formats for people with disabilities by calling 651-296-6753 or the Minnesota State Relay Service at 711 or 1-800-627-3529 (TTY). Many House Research Department publications are also available on the Internet at: www.house.mn/hrd/.

About The Internet and Public Policy Series

The Internet is a worldwide communication web created through technology, hardware and software, and human use patterns, which are shaped by mores, customs, and occasionally laws. States have their own roles within the larger national and international network that is the Internet. The challenge for policymakers is that the Internet itself is malleable, and no static definition can capture its breadth and changing uses.

This series of information briefs isolates discrete policy issues and the ways in which specific Internet issues provide choices for the Minnesota marketplace and for lawmakers. See the list at the end of this document for other titles in this series.

Introduction

As the Internet expands the ways people interact, it also offers a new arena for illegal activities. Some of those activities are traditional crimes while others deal directly with the use of computers and software. For example, the Internet allows for greater access to victims of harassment and stalking.[1] It also offers new ways to access financial records to facilitate crimes like theft and fraud. Identity theft has found particularly fertile ground online: in 2001, the FTC documented 86,250 identity theft complaints and in 2015, that number had ballooned to 490,226.[2]

Criminals attempt to hide their actions by using new pathways for illegal transactions, or alternative payment methods like Bitcoin, which can be difficult to track.[3] Programmers, seeking personal gain or notoriety, create software that steals information from computers, locks them temporarily, or attempts to completely shut down large computer networks. Even seemingly simple acts like downloading music, photographs, and written materials may violate copyright laws.[4]

Lawmakers have addressed the use of computers by amending existing laws to specifically include actions taken over the Internet and creating new crimes where existing laws do not apply. But, even where crimes committed on the Internet fall under existing laws, there are challenges to prosecuting them. The Internet allows people to remain anonymous and can make it difficult to identify particular perpetrators.[5] There are few boundaries on the Internet and actions can easily cross county, state, and national borders, leading to questions about appropriate jurisdiction.[6]

This brief will discuss federal laws that have been enacted or expanded to address criminal conduct on the Internet and Minnesota laws that are specific to the Internet, as well as laws that apply to actions taken on the Internet.

Federal Laws with Criminal Penalties

Congress began addressing computer-related crimes in the 1980s. In the ensuing years, Congress has enacted laws dealing specifically with computer fraud, hacking, and communication privacy. In addition, Congress has criminalized some acts and expanded existing laws to apply to crimes involving information stored as an electronic document.

Early Federal Laws Addressed Computer Fraud

The first federal action related to computer fraud began in the 1980s. While existing laws clearly covered certain actions committed while using computers, crimes like theft or burglary required a physical trespass or the taking of physical property. Studies released in 1983 and 1984 led to legislation that expressly prohibited the unauthorized use of computers.[7] The initial legislation was narrow but later changes have expanded the prohibitions.

Congress passed major criminal legislation known as the **Comprehensive Crime Control Act of 1984**.[8] It, and later amendments, are the primary tools used to address hacking offenses. Within that larger piece of legislation were the first laws making it illegal to access certain computers without authorization.[9] The act prohibited using or accessing a computer without authorization in three specific situations:

(1) to obtain classified United States military or foreign policy information with the intent to use the information to harm the United States or help a foreign nation;
(2) to obtain financial or credit information that is protected under a federal financial privacy law; or
(3) to access a federal government computer and use, modify, destroy, or disclose any information or prevent others from using that computer.

The statute specifically gave the Secret Service investigative authority. Since 1984, Congress has amended the law many times.

The first major amendment to the 1984 law was the **Computer Fraud and Abuse Act (CFAA)**.[10] The new law, enacted in 1986, expanded the list of actions prohibited by United States Code, title 18, section 1030. The amendment included new definitions clarifying that the prohibitions applied to a person who accessed a computer without authorization or exceeded the scope of authorized access. A person "exceeds authorized access" when accessing a computer with authorization, but uses that access "to obtain or alter information in the computer that the accessor is not entitled to so obtain or alter."[11] In particular, the amendments criminalized certain property theft associated with computer fraud, altering or damaging data that belongs to others, and selling passwords or similar access information.[12] While broader in scope, Congress intentionally limited federal enforcement to cases involving a compelling federal interest.[13]

Congress has amended the CFAA multiple times since 1986.[14] The changes added a civil cause of action, expanded the conduct prohibited by the law, and increased penalties. In its current form, the CFAA criminalizes nine types of activity:

- obtaining national security information

- accessing a computer and obtaining information (1) in a financial record of a financial institution or a credit card issuer, (2) from any department or agency of the United States, or (3) from any protected computer including one used exclusively by a financial institution or United States government, or one which affects interstate or foreign commerce even if located outside of the United States
- trespassing in a government computer
- accessing a computer to defraud and obtain value
- intentionally damaging by knowing transmission of code or a program such as a computer virus
- recklessly damaging a protected computer by intentional access
- negligently causing damage and loss to a protected computer by intentional access
- trafficking in passwords if the passwords affect commerce or a computer used by the United States government
- extortion involving computers

Punishment for violations of the law range from one to ten years in prison for first-time offenders.[15] The Secret Service has retained investigation authority for violations of the law except that the Federal Bureau of Investigation has primary authority to investigate violations that involve espionage, foreign counterintelligence, national defense, or foreign relations.

The CFAA is the government's primary tool in addressing computer hacking.[16] Courts have read the provisions that establish violations based on obtaining information from a protected computer broadly, noting that obtaining information includes merely reading that information.[17] In effect, any information received through the Internet meets one of the elements for violations of the CFAA. Similarly, protected computers include any that affect interstate commerce, and courts have noted that all computers connected to the Internet affect interstate commerce.[18] Any contact between an individual's computer and an Internet website will constitute obtaining information from a protected computer. Limitations to the law focus on other elements including whether violating a website's terms of use or corporate computer use restrictions constitute exceeding unauthorized access[19] or what acts constitute "damage."[20]

Federal Action Also Included Addressing Communication Privacy

During the 1980s, Congress also adopted the **Electronics Communications Privacy Act (ECPA)**, which included the **Stored Communications Act (SCA)**.[21] The acts updated the **Federal Wiretap Act of 1968**, which addressed the interception of telephone conversations. The new laws expanded the protections to all wire, oral, and electronic communications while they are being made, transmitted, or stored on a computer. As a result, the law covered e-mail and data stored electronically. Like the CFAA, the laws have been amended several times.[22]

The ECPA consisted of three separate sections. The first, Title I, is known as the Wiretap Act.[23] That section prohibits:

- intercepting or attempting to intercept any wire, oral, or electronic communications;
- using an electronic, mechanical, or other device to intercept oral communications;

- disclosing or attempting to disclose the contents of any wire, oral, or electronic communication knowing that the information was obtained through the interception of communications;
- using or attempting to use the contents of any wire, oral, or electronic communication knowing that the information was obtained through the interception of communications;
- intentionally disclosing or attempting to disclose the contents of communications intercepted legally knowing that the information was intercepted in connection with a criminal investigation; and
- electronic communication service providers from divulging the contents of a communication being transmitted.

The Wiretap Act contains multiple exceptions: allowing interception by operators, service providers, and FCC employees to perform work that is necessary to providing service; individuals who are a party to the communication or who have received prior consent from one of the parties; interception of communications, like radio broadcasts, which are readily accessible to the public; and law enforcement to intercept communications with an appropriate warrant or consent. Violations of the Wiretap Act are felonies and can be punished by up to five years in prison.

Several courts have read the term "intercept" narrowly, finding that the interception must be contemporaneous with the communication.[24] Other courts have expanded this requirement slightly allowing prosecution when the receiving computer duplicates an e-mail and forwards it.[25]

Title II of the ECPA is the Stored Communications Act.[26] The SCA applies to files and records held by service providers and makes it illegal to obtain, alter, or prevent authorized access to electronic communication that is in storage without authorization. Exceptions include allowing providers to disclose communications to the intended recipient or with that recipient's lawful consent. Violations can be punished with a prison sentence of up to ten years.

The SCA contains exceptions. The government can require the disclosure of electronic communications in some cases. If the communication has been in storage for 180 days or less, the government must obtain a warrant. If the communications have been in storage for over 180 days, the government can provide notice to the customer and then issue a subpoena to obtain the records. However, providers must turn over basic identification information to the government when receiving a subpoena, including the name, address, telephone records, and payment records.

The **USA PATRIOT Act** provided the FBI with additional administrative powers to obtain records without a warrant.[27] Under the law, the FBI can request the name, address, length of service of a customer, and local and long distance toll billing records when the agency certifies in writing that the records sought are relevant to an authorized investigation to protect against international terrorism. The law does not authorize disclosure of the content of any communications.[28]

The third provision of the ECPA relates to pen registers and trap-and-trace devices.[29] That section requires law enforcement to obtain court orders before installing devices that capture

dialed numbers or ones that capture the numbers from incoming calls. Violation of that requirement can be punished by up to one year in prison.

Congress Has Criminalized Certain Acts and Broadened Existing Laws to Apply to Electronic Documents

In addition to the broad legislation passed to address electronic communications, Congress also adopted several narrower laws designed to criminalize particular acts. The Credit Card Fraud Act of 1984 addresses unauthorized devices, including account numbers, that can be used to transfer money.[30] Congress expanded the law to also cover the interception of wire or electronic transmissions of telecommunications services.[31]

The **Economic Espionage Act** criminalizes the misappropriation of trade secrets.[32] Prior to the act, prosecutors attempted to use the Interstate Transportation of Stolen Property Act to prosecute similar offenses.[33] However, that law was not designed to apply to intellectual properties and thefts had increased as a result of new information technologies.[34] Title V of the act also required the courts and United States Sentencing Commission to provide reports on the use of encryption or scrambling technology used to facilitate or conceal crimes when that action would qualify for a sentence enhancement under section 3C1.1 of the U.S. Sentencing Guidelines.

The **Identity Theft Assumption and Deterrence Act of 1998** criminalizes producing, possessing, or transferring an identification document, authentication feature, or false identification document.[35] The law specifically addresses copying or transferring a prohibited item by electronic means. Addressing fraud associated with mass e-mails, Congress criminalized activities connected to sending multiple commercial e-mail addresses.[36] The Identity Theft Penalty Enhancement Act of 2004 created a penalty enhancement for a person who impersonates someone while committing specific felony offenses including mail, bank, and wire fraud.[37]

Other federal laws have undergone minor changes to clarify that they apply to electronic actions or documents. The prohibition on counterfeiting foreign obligations or securities added a provision related to electronic copies.[38] Definitions in criminal fraud in relation to identification documents expanded to include computer and electronic developments.[39] The criminalization of copyright infringement expanded to include electronic copies.[40] Sentence enhancements that applied to telemarketing added a reference to e-mail marketing.[41]

Expansions have also focused on sexual violence. Congressional findings introducing the **Child Pornography Prevention Act of 1996** stated that the law was necessary based in part on a finding that "new photographic and computer imaging technologies make it possible to produce by electronic, mechanical, or other means, visual depictions of what appear to be children engaging in sexually explicit conduct."[42] That statute added a new definition of child pornography to expressly cover electronic images. A related act in 2003 addressed visual representations of the sexual abuse of children, including computer-generated images.[43] The Violence Against Women Reauthorization Act of 2013 added a specific provision related to the use of an interactive computer service or electronic communication service to harass, threaten to kill, place under surveillance, or otherwise intimidate another person.[44]

Other actions may constitute crimes under existing statutes even in the absence of a direct reference to electronic communications. Actions like those that threaten, harass, or involve blackmail are not made legal simply because the conduct takes place over the Internet. Prosecutors are free to charge individuals with crimes for those actions.

Prosecutors cannot charge someone simply for violating the terms of use on a website. However, those restrictions often include items that can constitute a crime such as:

- impersonating another person or business;
- posting pornography or other sexually explicit images;
- defaming another;
- harassing, stalking, threatening, or bullying others; or
- releasing another's confidential information.

There are ongoing debates about whether website hosts should share liability for users' crimes. The Communications Decency Act provided providers with broad protection from civil suits related to online posts generated by users.[45] Those protections do not apply to criminal actions. Following some high-profile crimes involving classified ads on Craigslist.com, some sources called for imposing criminal penalties on website hosts.[46] While no laws have imposed such penalties to date, legislation has been proposed to specifically establish criminal penalties for a host that allows itself to be used to promote sex trafficking.[47]

While the federal government has taken action to address criminal activity involving computers, some of that action may be ineffective. Information shared between computers easily crosses state and even most national borders and legislation in the United States and other countries remained piecemeal for decades. The **2001 Convention on Cybercrime** sought to create a common criminal policy to address cybercrime.[48] Thirty countries, including 26 European countries, the United States, Canada, Japan, and South Africa, signed the treaty.[49] The treaty called for each signatory to adopt laws addressing concerns including offenses against computer data and systems, computer forgery and fraud, child pornography, and copyright infringement. The United States Senate ratified the treaty in 2006.[50] While the treaty is binding, it identifies areas in which countries must adopt legislation without providing specific required language.

Minnesota Criminal Laws Related to Computer Access and Online Conduct

Minnesota passed or expanded several laws to directly address crimes committed on the Internet. Some crimes, or portions of the crimes, are specific to the Internet. The statutes cover a wide range of activities from illegal ticket purchases to the nonconsensual dissemination of private sexual images ("revenge porn").

Minnesota Statutes, section 609.527, is Minnesota's identity theft law. Subdivision 5a makes it a felony to use false pretenses in a communication on the Internet in an attempt to obtain the identity of another person. The act is a crime even if only attempted or if the actor did not use the identity.

It is illegal to interfere with an emergency call under Minnesota Statutes, section 609.78. In 2013, Minnesota expanded the definition of "call" to include e-mails, calls made over the Internet using Voice over Internet Protocols, and the electronic transmission of an image or video.

Since 2008, Minnesota Statutes, section 609.806, has made it a crime to interfere with Internet ticket sales by using or selling software to circumvent security measures on a ticket seller's website designed to assure a fair ticket-buying process.

One of the most comprehensive laws addressing new technology addresses the nonconsensual dissemination of private sexual images. The law, Minnesota Statutes, section 617.261, is known as Minnesota's "revenge porn" law. It is illegal to share images of other people when the subject is identifiable, the subject did not consent to the image being shared, and the image was obtained under circumstances in which the subject had a reasonable expectation of privacy. It is a crime to share the images in a way that does not involve the Internet, but posting the image on a website, or maintaining a website or application for the purpose of sharing the image, enhances the crime to a felony. The law also specifically addresses the Internet by creating immunity for services and providers who make it possible to share the image.

State Laws Encompass Illegal Actions that Take Place on the Internet

Many laws do not require any modification to apply to actions taken on the Internet. For example, if a person uses the Internet to commit a theft, the action is still a theft. The Internet has not dramatically changed the basic premise of most crimes, but it is particularly relevant to existing crimes involving online bullying and computer-related offenses.

Harassment and stalking. Crimes like harassment and stalking are not specifically tied to the Internet, but the Internet provides an easy avenue for repeatedly contacting someone and for sharing statements to a wide audience.

Both harassment and stalking exist outside of the Internet but do not require any direct contact, and actions that take place only on the Internet can be criminal.[51] Harassment covers a wide range of conduct including the dissemination of private sexual images under the "revenge porn" law and repeated intrusive or unwanted acts that adversely affect the safety, security, or privacy of another. Under Minnesota Statutes, section 609.79, it is illegal to use a telephone to send obscene or harassing messages by telephone. The original version of the law went into effect in 1963 but a person could use a cell phone to send obscene messages over the Internet and violate this statute. A person who is the subject of harassment can obtain a restraining order under Minnesota Statutes, section 609.748, and a violation of that order is a crime.

Stalking, illegal under Minnesota Statutes, section 609.749, includes actions that make a victim feel threatened, intimidated, or persecuted. Monitoring someone and repeatedly contacting them can rise to the level of stalking.

Crimes involving computers. Several crimes involving computers apply to actions taken in person or over the Internet. Minnesota Statutes, section 609.88, criminalizes computer damage.

That damage includes distributing destructive programs such as a computer virus. That provision appeared in 1989, two years before the Internet went public.[52] It would apply to distribution through the Internet.

It is illegal to steal a computer under Minnesota Statutes, section 609.89. Originally, the statute made it illegal to deprive the owner of possession but a 1994 amendment made it illegal to deprive the owner of the use of the computer. That provision would apply to ransomware attacks sent over the Internet.[53] Minnesota Statutes, section 609.8912, addresses similar behavior by prohibiting the use of encryption without specifying whether the encryption involves the Internet.

Accessing a computer without authorization and facilitating access to a computer security system are both crimes. (Minn. Stat. §§ 609.891 and 609.8913) The statutes do not require that the access be in person and therefore covers hacking or other actions taken over the Internet.

Provisions in some laws do not create a crime, but acknowledge the role of the Internet. For example, Minnesota Statutes, section 243.055, allows conditions of supervision for a person on probation, parole, or supervised release to include limiting or prohibiting Internet access. Other statutes specifically address the question of where a case should be prosecuted by expanding the appropriate venue to either the place where a person allegedly took a criminal action or at the place where the victim suffered an injury.[54]

Other Works in the Series

This series of information briefs isolates discreet policy issues and the ways in which specific Internet issues provide choices for the Minnesota marketplace and for lawmakers. The following publications are part of the Internet and Public Policy series:

- Challenges and policy consideration for state regulation
- Privacy and consumer protection
- Cybertorts and property rights online
- Jurisdiction and procedures in Internet law cases
- Federal Internet laws
- State and federal accessibility laws

There may be more topics added, as needed. A special attempt will be made to keep all of these pieces up to date, but the pace of change may prove challenging.

ENDNOTES

[1] Alice Marwick and Ross Miller, *Online Harassment, Defamation, and Hateful Speech: A Primer of the Legal Landscape*, Center on Law and Information Policy at Fordham Law School, http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1002&context=clip.

[2] Federal Trade Commission, *Consumer Sentinel Network Data Book for January – December 2016* (March 2017); https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf.

[3] Joshua Bearman, "The Rise & Fall of Silk Road, Part I;" *Wired*, May 2015, https://www.wired.com/2015/04/silk-road-1/.

[4] Anita B. Froblich, "Copyright Infringement in the Internet Age – Primetime for Harmonized Conflict-of-Laws Rules," *Berkeley Technical Law Journal* vol. 24 (2009): 851. Available at: http://scholarship.law.berkeley.edu/btlj/vol24/iss2/5.

[5] Kristin Finklea and Catherine A. Theohary, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*, Congressional Research Service (2015), https://fas.org/sgp/crs/misc/R42547.pdf.

[6] Dr. Adel Azzam Saqf Al Hait, "Jurisdiction in Cybercrimes: A Comparative Study," *Journal of Law, Policy and Globalization*, vol. 22 (2014).

[7]Joseph B. Tompkins, Jr., and Linda A. Mar, "The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem," *Computer Law Journal*, vol. 6 (1986): 459. Available at: https://repository.jmls.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1512&context=jitpl.

[8] Pub. L. No. 98-473.

[9] 18 U.S.C. § 1030.

[10] Pub. L. No. 99-474.

[11] *Id*. at § 1030(e)(6).

[12] See, "Prosecuting Computer Crimes: Computer Crime and Intellectual Property Section Criminal Division," Department of Justice Office of Legal Education, Executive Office for United States Attorneys (2010). Available at: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

[13] Samantha Jensen, "Abusing the Computer Fraud Abuse Act: Why Broad Interpretations of the CFAA Fail," *Hamline Law Review*, vol. 36, iss. 1, art. 5. Available at: https://digitalcommons.hamline.edu/cgi/viewcontent.cgi?article=1008&context=hlr.

[14] Minor and Technical Criminal Law Amendments Act of 1988, Pub. L. No. 100-690 (1988); Financial Institutions Reform, Recovery, and Enforcement Act of 1989, Pub. L. No. 101-73 (1989); Financial Institutions Anti-Fraud Enforcement Act of 1990, Pub. L. No. 101-647 (1990); Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322 (1994); National Information Infrastructure Protection Act of 1996, Pub. L. No. 104-294 (1996); USA PATRIOT Act of 2001, Pub. L. No. 107-56 (2001); Criminal Law Technical Amendments Act of 2002, Pub. L. No. 107-273 (2002); Cyber Security Enhancement Act of 2002, Pub. L. No. 107-296 (2002); Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110-326 (2008).

[15] The United States Sentencing Commission amended its guidelines pursuant to direction from Congress in the Cyber Security Enhancement Act of 2002. Those changes included enhancements targeting offenses that involved the intent to obtain personal information, crimes committed with malicious intent, and crimes involving computer systems used in critical infrastructure, administration of justice, and national defense and national security. See *Report to the Congress*: *Increased Penalties for Cyber Security Offenses* (May 2003), available at: https://www.ussc.gov/sites/default/files/pdf/news/congressional-testimony-and-reports/computer-crime/200304_RtC_Increased_Penalties_Cyber_Security.pdf.

[16] Andrea Peterson, "This '80s-era Criminal Hacking Law Scares Cybersecurity Researchers," *The Washington Post* (August 5, 2015). Available at: https://www.washingtonpost.com/news/the-switch/wp/2015/08/05/this-80s-era-criminal-hacking-law-scares-cybersecurity-researchers/?utm_term=.eebdd3d3758f.

[17] *U.S. v. Drew*, 259 F.R.D. 449 (C.D.Cal. 2009).

[18] *Id.*; *U.S. v. Trotter*, 478 F.3d 918 (8th Cir. 2007).

[19] Courts have reached inconsistent conclusions on this question; *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) holding that the phrase "exceeds authorized access" does not extend to violations of use restrictions; *U.S. v. John*,

597 F.3d 263 (5th Cir. 2010) holding that violating an official corporate policy met the concept of "exceeds authorized access."

[20] *U.S. v. Keys*, 703 Fed. Apprx. 472 (9th Cir. 2017) temporary removal of an online article constitutes damage even when the original is not destroyed; *Turner v. Hubbard Systems, Inc.*, 855 F.3d 10 (1st Cir. 2017) to state a claim for a civil action, damages must generally be at least $5,000.

[21] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508.

[22] Communications Assistance to Law Enforcement Act of 1994, Pub. L. No. 103-414 (1994); USA PATRIOT Act of 2001, Pub. L. No. 107-56 (2001); USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 (2005); FISA Amendments Act of 2008, Pub. L. No. 110-261.

[23] 18 U.S.C. §§ 2510-2522.

[24] See, *U.S. v. Steiger*, 318 F.3d 1039 (11th Cir. 2003); *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3rd Cir. 2003); *Owen v. Cigna*, 188 F.Supp.3d 790 (N.D. Ill. 2016).

[25] *U.S. v. Szymuskiewcz*, 622 F.3d 701 (7th Cir. 2012).

[26] 18 U.S.C. §§ 2701-2712.

[27] USA PATRIOT Act of 2001, Pub. L. No. 107-56, Title V, Sec. 505 (2001); 18 U.S.C. § 2709.

[28] Title II, section 215 of the USA PATRIOT Act (50 U.S.C. § 1861 et seq.) allows the FBI to obtain search warrants for any records or other tangible things through the Foreign Intelligence Surveillance Act (FISA) court. The FISA court process is not public has been criticized as lacking transparency. However, after some debate, the USA PATRIOT Improvement and Reauthorization Act of 2005 did not give the FBI administrative powers to request those items without applying for a warrant.

[29] 18 U.S.C. §§ 3121-3127.

[30] Pub. L. No. 98-473; 18 U.S.C. § 1029.

[31] Court Enforcement of Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414.

[32] Economic Espionage Act of 1996, Pub. L. No. 104-294; 18 U.S.C. § 11030; 18 U.S.C. §§ 1831-1839; 18 U.S.C. § 4243.

[33] 18 U.S.C. §§ 2314-2315.

[34] Spencer Simon, "The Economic Espionage Act of 1996," *Berkeley Technical Law Journal*, vol. 13 (1998): 305. Available at: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1174&context=btlj.

[35] Identity Theft Assumption and Deterrence Act of 1998, Pub. L. No. 105-318; 18 U.S.C. § 1028.

[36] Controlling the Assault of Nonsolicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), Pub. L. No. 108-187.

[37] Identity Theft Penalty Enhancement Act of 2004. Pub. L. No. 108-275; 18 U.S.C. § 1028A.

[38] 18 U.S.C. § 481, amended by the USA PATRIOT Act of 2001.

[39] 18 U.S.C. § 1028, amended by the Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318.

[40] 17 U.S.C. § 506 and 18 U.S.C. § 2319, amended by the No Electronic Theft (NET) Act of 1997, Pub. L. No. 105-147.

[41] 18 U.S.C. § 2326, amended by the Elder Abuse Prevention and Prosecution Act of 2017, Pub. L. No. 115-70.

[42] Child Pornography Prevention Act of 1996, Pub. L. No. 104-208; 18 U.S.C. § 2251.

[43] Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act of 2003 (PROTECT Act). Publ. L. No. 108-21; 18 U.S.C. § 1466A.

[44] Pub. L. No. 113-4; 18 U.S.C. § 2261A.

[45] Telecommunications Act of 1996, Title V, Pub. L. No. 104-104; 47 U.S.C. § 230.

[46] Shahrzad T. Radbod, "Craigslist – A Case for Criminal Liability for Online Service Providers," *Berkeley Technical Law Journal*, vol. 25 (2010): 597. Available at: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1838&context=btlj.

[47] Tom Jackman, "Senate Launches Bill to Remove Immunity for Websites Hosing Illegal Content, Spurred by Backpage.com," *The Washington Post* (August 1, 2017). Available at: https://www.washingtonpost.com/news/true-crime/wp/2017/08/01/senate-launches-bill-to-remove-immunity-for-websites-hosting-illegal-content-spurred-by-backpage-com/?utm_term=.6efe0aaa66e1.

[48] Convention on Cybercrime, Budapest. Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

[49] Sarah Left, "Thirty Countries Sign Cybercrime Treaty," *The Guardian*, November 23, 2001. Available at: https://www.theguardian.com/technology/2001/nov/23/Internetnews.

[50] Senate Treaty Document No. 108-11.

[51] See, *Johnson v. Arlotta*, 2011 WL 6141615 (Dec. 12, 2011) posting a blog about a former girlfriend constituted harassment; *State v. Hennessy*, 2012 WL 2505889 (July 2, 2012) using the Internet to engage in stalking behavior.

[52] Tony Long, "Aug. 7, 1991: Ladies and Gentlemen, The World Wide Web," *Wired* (2007), https://www.wired.com/2012/08/aug-7-1991-ladies-and-gentlemen-the-world-wide-web/.

[53] Ransomware is a virus that encrypts a person's computer and demands payment in return for the decryption code. While ransomware is not new, its spread on the Internet is relatively recent. Alina Simone, "Ransomware's strange history began with a colourful culprit," *Toronto Star*, May 17, 2017, https://www.thestar.com/news/insight/2017/05/17/ransomwares-strange-history-began-with-a-colourful-culprit.html.

[54] See Minn. Stat. §§ 609.527, subd. 6; 609.79, subd. 2; and 609.749, subd. 1b.