TYPES OF CYBERCRIMES ©

SEARCH AND SEIZURE OF COMPUTERS AND DIGITAL EVIDENCE
February 2009

by

PRISCILLA GRANTHAM ADAMS
Senior Research Counsel

National Center for Justice and the Rule of Law
The University of Mississippi
School of Law
University, MS 38677
Phone: (662) 915-6897 Fax: (662) 915-6833
www.NCJRL.org

© Copyright 2009 National Center for Justice and the Rule of Law - All rights reserved
INTRODUCTION
Computers are an integral part of daily life. The term “computer” encompasses more than the typical desktop or laptop machine. As technology evolves, so do the forms, sizes, shapes and uses of computers. Regardless of the varied appearance of computers, they are all digital devices; they process and store information as data in binary form (1's and 0's).

There is not a standard definition for the term Cybercrime. It is sometimes referred to as “Computer Crime,” “High tech crime,” “Internet crime,” and Information Age crime” to name a few. It is helpful to think of cybercrime as any crime in which a computer or other digital device is involved, regardless of whether the crime fits under any statutory definition of computer crime. Building on this, cybercrime can be defined by reference to the three ways in which computers can be involved in crime: Target, Tool, or Container.

I. COMPUTER AS TARGET

A. Crimes in which computers are the target are thought of as “true computer crimes.” These are crimes that did not exist before the spread of computer technology and computer networks. The Computer Fraud and Abuse Act 18 U.S.C. § 1030 (2000) and its amendments under the USA PATRIOT Act of 2001 is the primary federal statute aimed at combating computer crime. The CFAA applies to conduct aimed at a “protected computer,” which is any computer connected to the Internet. Additionally, many states have their own Computer Crime Acts.

B. Target Crimes

■ Unauthorized Access
- Hacking - gaining unauthorized access to a computer
- Cracking - (aggravated hacking) - gaining unauthorized access to a computer to commit another crime, such as theft or vandalism.

■ 18 U.S.C. § 1030(a)(5) targets what is commonly referred to as computer hacking and prohibits:
  ■ knowingly causing the transmission of a program, information code, or command and intentionally causing damage to a protected computer; or
  ■ intentionally accessing a protected computer and recklessly causing damage; or
  ■ intentionally accessing a protected computer and negligently causing damage.

■ The following acts were found to be violations under 1030(a)(5):
  ■ releasing a worm that caused computers at various educational and
military institutions to cease functioning
- former bank employee damaged files by accessing and viewed files using old password to log onto mainframe
- ex-computer administrator employee hacked into company’s email program enabling him to change administrative passwords, alter computer’s registry, and delete billing system and internal databases

**Computer Sabotage** is a type of unauthorized access whereby a hacker releases or installs a virus, worm, logic bomb, or Trojan horse that in turn damages a computer or network.

- Virus - computer program, usually made to spread from computer to computer, that is intended to annoy the user or cause harm to his or her computer. A virus might place an annoying message on a computer or it might re-format the user’s hard drive, causing a loss of all data on the hard drive.

- Worm - a type of virus that self replicates over a network.

- Logic Bomb - a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met or at a specified time. Logic bombs do not self replicate.

- Trojan horse - a destructive program that masquerades as a benign application, for example, a program that claims to rid your computer of viruses, but instead introduces viruses onto your computer. Trojan horses are broken down in classification based on how they breach the systems and the damage they do. Some of the most pervasive and destructive Trojan horse programs launch Denial of Service (DoS) attacks by flooding a network with so many requests that regular traffic to the targeted website is interrupted.

**State Computer Crime Statutes** -
As technology continues to evolve and advances are made with ever increasing rapidity, states tend to promulgate and adopt technology-specific crime laws, even when there are existing laws that encompass the particular situation. The result is that a defendant may be prosecuted under a “name-brand” law when a charge under a “generic” law is available, and perhaps preferable. For example, in *People v. Rice*, 2008 WL 2053490, a defendant used a computerized phone system to make biweekly claims for unemployment benefits. When the system asked if she had worked during

---


the week for which she was claiming benefits, she entered ‘9’ for ‘no,’ even though she had been working. She was charged with and convicted under Colorado’s computer crime statute. While the defendant’s act (calling into the system for the purpose of obtaining money to which she wasn’t entitled) fit within the language of the statute, her conduct could have been prosecuted as ordinary fraud - she obtained property by tricking someone into giving it to her. This is an important point to remember, especially in cases where there might not be a specific computer crime statute on point.

Every state has enacted some form of computer specific legislation. In most states, simple hacking and aggravated hacking are treated as two distinct crimes, with simple hacking classified as a misdemeanor and aggravated hacking a felony. There are, however, other definitional variations among states statutes in the characterization of computer crimes. Depending on the jurisdiction, an act may be referred to as unauthorized access, computer trespass, unauthorized use, or computer tampering. For example, when an angry computer programmer deleted code from his company’s computer, he was found guilty of violating Georgia’s computer trespass statute, GA. CODE ANN. § 16-9-93 (1999). Fugarino v. State, 531 S.E.2d 187 (Ga. App 2000).

- Some states specifically criminalize the use of a computer to engage in other

---

4 COLO. REV. STAT. § 18-5-5-102(c)-(d) (   ). This statute provides in part:
A person commits computer crime if the person knowingly
. . .
(c) Accesses any computer, computer network, or computer system, or any part thereof to obtain, by means of false or fraudulent pretenses, representations, or promises, money; property; ... or other thing of value; or
(d) Accesses any computer, computer network, or computer system, or any part therein to commit theft. ...


7 ARK. CODE ANN. § 5-41-103 (Michie 1997), N.Y. PENAL LAW § 156.10 (McKinney 1998).


9 ARIZ. REV. STAT. ANN. § 13-2316 (West 2000).
criminal acts.\textsuperscript{10}

- A number of states criminalize the dissemination of viruses, worms and other malware.\textsuperscript{11}

- Many states have specific statutes criminalizing denial of service attacks\textsuperscript{12} and attempted denial of service attacks\textsuperscript{13}, while other states include denial of service in statute prohibiting distribution of malware.\textsuperscript{14}

\textbf{Theft of Data} - Unauthorized taking of sensitive, proprietary, or other intellectual property stored on a personal, govt., or corporate computer. Includes softlifting, software counterfeiting, warez, etc.

- \textbf{Softlifting} - illegal practice of taking one purchased piece of software and loading it onto multiple machines or a home computer in addition to a work machine in violation of the licence agreement.

- \textbf{Warez} - refers primarily to copyrighted works traded in violation of copyright law. Generally refers to releases by organized groups, as opposed to peer-to-peer sharing between friends or large groups of people using a darknet. It usually does not refer to commercial, for-profit software counterfeiting. Usually a noun, as in “My roommate downloaded 40 gigabytes of warez yesterday”; but has also been used as a verb, as in “The new version of Windows was warezed a month before it was officially released.”

- \textbf{Software piracy} - copyright infringement; creating a copy and or selling or giving it away.

\textbf{Theft of Services} - knowingly accessing a computer network without authorization.

\textsuperscript{10} ARK. CODE ANN. § 5-41-103 (Michie 1997), DEL. CODE ANN. tit. 11 § 2738 (2004), IDAHO CODE § 18-2202 (Michie 1997).


\textsuperscript{14} S.C. CODE ANN. § 16-16-10(k)(3) (Law Co-op. Supp. 2004).
Laws regarding the unauthorized access to a computer network exist in the federal government and all 50 states, but the interpretation of terms like “access” and “authorization” is not clear and there is no general agreement as to whether piggybacking (intentional accessing of an open Wi-Fi network without harmful intent) falls under this classification.

### Spam

  
  The CAN-SPAM Act was enacted to establish a national standard for email solicitations. It does not prohibit spam, but rather provides persons and businesses with a framework regarding sending commercial solicitations via email.

  - **CANNOT:**
    - send message in a way that the recipient can’t trace back to the sender;
    - send sexually explicit material without a warning label;

  - **CAN** send unsolicited email to anyone if:
    - the sender identifies himself;
    - they do not use fraudulent headers;
    - upon request, they stop sending the emails (opt out provision)

- **State Anti Spam laws**
  - **Scope** - At least thirty-six states have anti-spam laws. The provisions vary widely in scope; some of which are preempted by the federal Act. The scope of the preemption is not entirely clear, as it requires interpretation of the Savings Clause. What we do know is that the CAN-SPAM Act does not preempt state laws to the extent that they relate to fraud, false advertising, or trespass.
  - **Classification** - Violations of state spam statutes are usually a misdemeanor, unless there are a specified number of recipients in a given time period. Some state spam statutes provide that violation is a felony if there is a specified amount of revenue generated by a spam transmission.
  - **Jurisdiction** - Look to the language of the statute; it will set forth the requirements that need to be met to confer jurisdiction.

---

II. COMPUTER AS TOOL

Introduction - Almost any kind of traditional crime can be assisted through the use of computers or the Internet. While some offenses are unique to computers and require prosecution under statutes specific to computer operation and related activities, traditional, generic statutes apply and are used to prosecute many computer related offenses.

A. Statutes - Aside from the CFAA, there are at least forty other federal statutes that can be used to prosecute computer-related crimes. Ryan P. Wallace et al., Computer Crimes, AM. CRIM. L. REV., SPRING 2005, at 237. Additionally, every state has enacted some sort of computer-specific legislation.

B. Crimes utilizing computers:
- child pornography / child exploitation
- piracy - copyright infringement
- extortion - transmitting in interstate or foreign commerce any threat to cause damage to a protected computer with the intent to extort something of value.
- fraud, including scams perpetrated via phishing and spoofing
- swatting
- identity theft
- bullying
- stalking/harassment

Child Pornography - Federal law, as well as laws in every state, make the production, sending/distribution, receipt, and possession of child pornography a crime.

- CPPA, - Child Pornography Prevention Act of 1996 is the primary federal child pornography statute. It outlaws the production, receipt, transportation, and possession of child pornography through all means including computers. The Act has been modified through subsequent amendments and narrowed by Ashcroft, which held that child pornography must be of actual children rather than virtual images.

---

16 18 U.S.C. § 2252A

17 Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002) (Plaintiffs challenged portions of the CPPA act that expanded prohibitions against child pornography to include (1)“any visual depiction...that is, or appears to be, of a minor engaged in sexually explicit conduct”, and (2) sexually explicit images that are promoted or advertised in a manner that “conveys the impression” that the images depict a minor engaged in sexually explicit conduct. The Supreme Court held that these prohibitions on virtual child pornography are substantially overbroad and unconstitutional under the First Amendment.)
Child pornography:
- a visual depiction
  - of sexually explicit conduct*
  - using a minor (under 18) engaging in the conduct, or
  - digital or computer generated image that is, or is indistinguishable from, a
    minor, or
  - created or modified to appear that an identifiable minor is engaging in the
    act.

* Sexually explicit conduct:
  (1) Sex acts:
    Actual or simulated:
    - sexual intercourse (genital-genital, oral-genital, anal-genital, or
      oral-anal, between person of same or opposite sex)
    - bestiality
    - masturbation
    - sadistic or masochistic abuse, or
  (2) Lascivious exhibition of genitals or pubic area. (Nudity is not a
    requisite factor in the determination that a depiction is lascivious.)

  Factors considered in determining nature of images:
  - focal point (genitals or pubic area)
  - sexually suggestive setting
  - child in unnatural pose or inappropriate clothing
  - child fully or partially clothed, or nude
  - suggests coyness or willingness to engage in sexual activity
  - intended to elicit sexual response in viewer

PROTECT Act - Prosecutorial Remedies and Tools Against the Exploitation
of Children Today Act (2003). This Act makes it an offense to possess,
manufacture, or distribute pornography containing visual depictions of:
- a real child engaging in sexual acts, or
- a digital, computer, or computer-generated image that is, or is
  indistinguishable from, that of a minor engaged in sexually explicit
  conduct.

---

18 United States v. Knox, 32 F.3d 733 (3rd Cir. 1994).

Virtual Child Pornography - The Supreme Court held in Ashcroft\textsuperscript{20} that virtual child pornography is protected; it is not enough that the image appears to be of a minor, the image must be one of a minor or one that is indistinguishable from a minor.

- The issue as to whether the image is of a real child is a jury question.\textsuperscript{21} It is only necessary that an ordinary person would conclude that the depiction is of an actual minor engaged in sexually explicit conduct.

- Factors used to resolve real v. virtual question include:
  - the picture
  - known images database from NCMEC
  - what does suspect call pictures? Titles, labels, etc.
  - website memberships
  - volume of images
  - evidence of trading
  - expert testimony:
    - medical expert / pediatrician (body fat, proportions)
    - digital imaging expert
    - photographic expert
    - economics of technology, i.e., it would be cost and time prohibitive to produce the number of images or the video in question due to the quality. -

\textbf{Pandering} - In \textit{U.S. v. Williams},\textsuperscript{22} the Supreme Court upheld the provision of the PROTECT Act that criminalizes the pandering or solicitation of child pornography.\textsuperscript{23}

- Nature of offense:
  - prohibits offers to provide and requests to obtain child pornography
  - does not require actual existence of child pornography.


\textsuperscript{21} United States v. Vig, 167 F.3d 443 (8th Cir. 1999).

\textsuperscript{22} United States v. Williams, 128 S.Ct. 1830 (2008).

\textsuperscript{23} Section 2252a(a)(3)(B) makes it a crime for any person to knowingly advertise, promote, present, distribute, or solicit through the mails or interstate or foreign commerce by any means, including by computer, any material or purported material in a manner that reflects the belief, or that is intended to cause another to believe, that the material or purported material is, or contains an obscene visual depiction of a minor engaging in sexually explicit conduct; or a visual depiction of an actual minor engaging in sexually explicit conduct.
crime is committed only when the speaker believes or intends the listener to believe that the subject of the proposed transaction depicts \textit{real} children. (An offer to provide or a request to receive virtual child pornography is not prohibited.)

- First Amendment implications:
  - Offers to give or receive what is unlawful to possess have no social value, and thus, like obscenity, enjoy no First Amendment protection. The pandering provision criminalizes only offers to provide or requests to obtain \textit{contraband} in the form of child obscenity, and child pornography involving actual children – the proscription of which is constitutional.
  - Since the government can ban fraudulent offers and offers to provide illegal products, it stands to reason that fraudulent offers to provide illegal products should, if anything, be doubly excluded from the protections afforded by the First Amendment.

### Piracy - Copyright Infringement


- The Digital Millenium Copyright Act, 17 U.S.C. § 1201-05 (2000), prohibits the use of computers and other digital devices to infringe against copyrights on traditional works, and the circumvention of technological measures used to protect copyrighted works.

### Fraud

This category encompasses a full panoply of deceitful schemes. Many of these crimes are simply age old schemes being committed through the use of the Internet, and fall under the prohibitions set forth in general fraud statutes. Aside from the Computer Fraud and Abuse Act and analogous state computer fraud statutes, certain criminal acts facilitated by the use of a computer may be covered by the Federal mail and wire fraud statute\textsuperscript{24} which prohibits the use of interstate mail or wire transmissions to further a fraudulent scheme to obtain money or property.

- There is not a uniform statutory approach among the states to address the problem of fraud committed through the use of digital devices.

- A substantial number of states prohibit using computers to commit fraud\(^{25}\)
- Some states classify computer fraud as a separate crime\(^{26}\)
- Some states include using a computer to commit fraud in their basic aggravated hacking statute\(^{27}\)
- Some states' statute provides statutorily for increased penalties for aggravated hacking if it was done in order to devise or execute a scheme to defraud\(^{28}\)

- The following acts were found to be a violation of the federal wire fraud statute:
  - Posting a fraudulent solicitation for money on a classified ad website,\(^{29}\)
  - Fraudulent transfer of funds through a computer system,\(^{30}\)
  - Alteration of computer clocks by government contractor to “backdate” reports, it appears they were completed during specified period,\(^{31}\)
  - Use of a computer program by a reseller of long distance phone service to add extra minutes to calls of customers\(^{32}\)


\(^{29}\) United States v. Pirello, 255 F.3d 728, 732 (9th Cir. 2001).

\(^{30}\) United States v. Briscoe, 65 F.3d 576, 580-81 (7th Cir. 1995).

\(^{31}\) United States v. Gaind, 31 F.3d 73, 75 (2d Cir. 1994).

\(^{32}\) Mid Atlantic Telcom, Inc. v. Long Distance Servs., Inc., 18 F.3d 260, 264 (4th Cir. 1994).
Identity Theft

- **The Internet False Identification Act of 2000**, 18 U.S.C. § 1028 prohibits the production, transfer, or possession in certain circumstances of false identification documents (or a document making implement with the intent to make a false id document) or identification documents that were not legally issued to the possessor. Also prohibits the making of software or data to make false identification available online.

- State Identity theft statutes, while not identical, generally prohibit:
  - intentional and non-consensual
  - misappropriation
  - of personal identification documents or information of another
  - in order to obtain a benefit or economic value.

- If a state does not have a statute aimed specifically at identity theft, there are other statutes under which the criminal conduct may be prosecuted, for example, forgery, theft, false impersonation, credit card fraud or access devise fraud.

- “MPOSTURE” - going on-line and pretending to be someone else. Can result in a variety of charges: defamation, identity theft, computer fraud, stalking/ harassment.

- A defendant who hacked into his boss’ email account and forwarded emails he found regarding an extramarital affair his boss was having was charged under Wisconsin’s identity theft statute, which criminalizes the whole act of using someone else’s identity without their permission for one of the enumerated purposes. Defendant’s conduct fit within the language of the statute in that he intentionally, without authorization, represented he was another person in order to harm that person’s reputation.

- Defendant went on-line and, pretending to be his former boss, posted an ad on a website that featured requests for sexual encounters. He gave a personal description, phone number, etc. Convicted for criminal defacement.

- Man created Facebook pages for two young women without their knowledge or consent. He then used their identities to have virtual sex with other men. He was charged under Indiana’s stalking and harassment statute, but this doesn’t seem to fit since the communications were not directed to the victims.

- “MySpace Suicide Case”
  How do we classify certain acts carried our by use of a computer? Lori Drew allegedly set up a profile of a young boy on MySpace and, pretending to be the boy, began chatting with Megan Meier in order to find out what Megan was saying about her daughter. Ms. Drew was charged with three counts of accessing
a protected computer without authorization to obtain information to inflict emotional distress on Megan Meier. The indictment alleges that Ms. Drew violated MySpace’s TOS agreement.

■ Stalking

• 18 U.S.C. 2261A (2000) prohibits the use of any facility of interstate or foreign commerce to engage in a course of conduct that places a person in reasonable fear or death or serious injury to themselves or a family member.

• State statutes - Every state and the District of Columbia has a statute that prohibits stalking. In at least twelve states, statutory language explicitly sets forth that electronic communications may constitute stalking. It is likely that forms of cyberstalking are also prohibited by state statutes that allow threats to be implied by conduct.

• Missouri Governor Matt Blunt signed a bill that updates the state’s stalking and harassment statutes. Vernon’s Annotated Missouri Statutes § 565.225.
  
  ■ under the bill, one could commit stalking by sending someone two or more email messages that serve no legitimate purpose and would cause a reasonable person under the circumstances to be “emotionally distressed.”
  ■ aggravated stalking if perpetrator is twenty-one or older and the victim is seventeen or younger. (Think Lori Drew.)

■ Cyber bullying

• Thirty six states have laws prohibiting bullying, cyber bullying, and harassment. See www.bullypolice.org for a list of states that have passed anti-bullying laws and applicable links.
  
  ■ Most of the states that have passed cyber bullying laws have written them to protect students and the school districts.
  ■ Some of the states’ laws apply only if the student was bullied by the use of a computer or electronic device belonging to the school, or if the offense takes place on school grounds.
  ■ several states have laws that protect the student even if the bullying occurs off-campus if it can be proven that the bullying is affecting the student’s ability to learn or is disruptive to the school.

• In May of 2008, U.S. Representatives Linda Sanchez (CA) and Rep. Kenny Hulshof (MO) co-sponsored legislation in Congress to make cyber bullying a federal crime, punishable by up to two years in prison.
The difficulty in writing bills that prohibit cyber bullying is in balancing the First Amendment rights of those engaging in various cruel behaviors against the need to protect those whom are adversely affected.

**Transmitting Threats / Harassment -**

- 18 U.S.C. § 875 (2000) prohibits transmitting the following communications in interstate or foreign commerce:
  - demand for ransom for the release of any kidnapped person;
  - intent to extort money;
  - threat to injure a person; or
  - threat to damage property

- What is a threat?
  - a reasonable person would find the communication to be a serious expression to inflict serious bodily injury; **and**
  - the communication was being communicated to effect a change or achieve a goal through intimidation.

- The court in *U.S. v. Alkhabaz*[^33], 104 F.3d 1492 (6th Cir. 1997) held that defendant did not violate 18 U.S.C. § 875 by exchanging emails with another in which they discussed the torture, rape and murder of a named classmate of the defendant. The court reasoned that the purpose of the emails was not to affect a change or achieve a goal through intimidation, but to foster a friendship based on shared interests.

**III. COMPUTER AS CONTAINER**

A computer may contain evidence of any traditional crime, even if it was not used in the commission of the crime. For example business records of a criminal enterprise may be stored in computer files. Email exchanges, driving directions, and search engine queries may all contain evidence of crimes. Metadata also can contain evidence; i.e. to whom a certain computer program is registered, make and model of camera used to take digital photographs.

[^33]: United States v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997).