

Cyberspace Law
H. Tomás Gómez-Arostegui
Fall 2006
Federal Cybercrime
Substantive

There are several federal statutes that cover computer crime. The elements of the most important statutes, and the possible penalties, are briefly described here. Most of these crimes may also be enforced by a private, civil cause of action; so I also list (when relevant) the elements for the civil causes of action. Indeed, because most criminal cases “plea out,” meaning they are decided on a guilty plea, most of the case law analyzing the provisions of these criminal/civil laws comes from civil cases. Though this handout is limited to federal laws, there are often state laws covering similar offenses. Those state laws often mimic the federal laws, and so I won’t describe them here. Also keep in mind that I have selected only certain federal criminal laws. This memorandum is not intended to be, and is not, an exhaustive statement of the elements of every cyber criminal law.

A. THE COMPUTER FRAUD AND ABUSE ACT

The Computer Fraud and Abuse Act (CFAA), *see* 18 U.S.C. § 1030, prohibits a variety of fraudulent activities occurring in connection with computers. The statute contains criminal penalties that may be sought by the U.S. Government and civil remedies that may be sought in a private, civil cause of action. Four potential claims/crimes are analyzed in the sections that follow.

1. Access Involving an Interstate Communication

Section 1030(a)(2)(C) of the CFAA prohibits a person from intentionally accessing certain computers remotely, without authorization, by using an interstate communication (such as by logging onto the computer via a phone line or the internet) in order to obtain information from the computer.

a. The Elements of the Claim/Crime

In order to state a civil claim under Section 1030(a)(2)(C), a plaintiff must demonstrate:

- (1) that the defendant intentionally accessed a computer without authorization or by exceeding authorized access;¹
- (2) that the defendant thereby obtained information from a protected computer;²

¹ The term “exceeds authorized access” means “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.” 18 U.S.C. § 1030(e)(6).

² A “protected computer” includes a computer “which is used in interstate or foreign commerce or communication.” 18 U.S.C. § 1030(e)(2). One court has held that computers connected to the Internet and that are

- (3) that the conduct involved an interstate or foreign communication;³
and
- (4) loss to 1 or more persons during any 1-year period aggregating to at least \$5,000 in value.

See 18 U.S.C. §§ 1030(a)(2)(C), (g). The criminal component of this section requires the same showing, with the exception that the loss requirement of element (4) is not required. See *id.* § 1030(a)(2)(C). Moreover, in a criminal case the elements must be proven beyond a reasonable doubt, rather than by a preponderance of the evidence.

b. Potential Civil and Criminal Remedies

In the event the plaintiff is able to make out a civil claim, the remedies would include compensatory damages (which are limited to economic damages) and injunctive or other equitable relief. See 18 U.S.C. § 1030(g). The CFAA does not award to the prevailing party attorneys' fees and does not provide for punitive damages. The potential criminal penalties and the classification of this offense (as a felony or misdemeanor) depend on the circumstances of the violation. The offense would be classified as a Class D felony, and violators would be subject to a fine and/or up to 5 years of imprisonment, if (1) the offense was committed for purposes of commercial advantage or private financial gain; (2) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or (3) the value of the information obtained exceeds \$5,000. See 18 U.S.C. §§ 1030(c)(2)(B), 3559(a)(4). If none of these circumstances is present, then the offense is classified as a Class A misdemeanor and any violators would be subject to a fine and/or a maximum of 1 year in prison. See *id.* §§ 1030(c)(2)(A), 3559(a)(6).

"used to send and receive e-mail . . . throughout the country[,] qualify as a protected computer under the CFAA." *Credential Plus, LLC v. Calderone*, 230 F. Supp. 2d 890, 906 (N.D. Ind. 2002).

³ "Interstate or foreign communication" is not defined in the U.S. Criminal Code. However, the Federal Communications Act defines "interstate communication" as a "communication or transmission from . . . any State, Territory, or possession of the United States (other than the Canal Zone), or the District of Columbia, to any other State, Territory, or possession of the United States (other than the Canal Zone), or the District of Columbia, . . . but shall not . . . include wire or radio communication between points in the same State, Territory, or possession of the United States, or the District of Columbia, through any place outside thereof, if such communication is regulated by a State commission." 47 U.S.C. § 153(22).

2. Access Involving an Intent to Defraud and Obtaining Something of Value

Section 1030(a)(4) of the CFAA generally prohibits a person from intentionally accessing a computer, without authorization, where that person has an intent to defraud and obtains something of value from the computer (such as trade secrets, for example).

a. The Elements of the Claim/Crime

In order to state a civil claim under Section 1030(a)(4), a plaintiff must demonstrate that:

- (1) the defendant knowingly and with intent to defraud;
- (2) accessed a protected computer without authorization or by exceeding authorized access;
- (3) by means of such conduct the defendant furthered the intended fraud and obtained anything of value (other than the use of the computer itself); and
- (4) loss to 1 or more persons during any 1-year period aggregating to at least \$5,000 in value.

See 18 U.S.C. §§ 1030(a)(4), (g). The criminal component of this section requires the Government to prove the same elements, with the exceptions, again, that the loss requirement of element (4) is not required, *see id.* § 1030(a)(4), and the elements must be proven beyond a reasonable doubt.

b. Potential Civil and Criminal Remedies

The civil remedies for a violation of this section of the CFAA are the same as stated above. See 18 U.S.C. § 1030(g). A criminal violation of this section is a Class D felony and is punishable by a fine and/or up to 5 years in prison. *See id.* §§ 1030(c)(3)(A), 3559(a)(4).

3. Access Impairing the Integrity or Availability of a System or Information

Sections 1030(a)(5)(ii) and (iii) of the CFAA generally prohibit a person from intentionally accessing a computer, without authorization, and in a way that causes damage to data, a program, the system, or information contained on the computer.

a. The Elements of the Claim/Crime

In order to state a civil claim under Sections 1030(a)(5)(A)(ii) and/or (iii), a plaintiff must demonstrate that the defendant:

- (1) intentionally accessed a protected computer without authorization;

- (2) their conduct caused damage, *i.e.*, impaired the integrity or availability of data, a program, a system, or information;⁴ and
- (3) loss to 1 or more persons during any 1-year period aggregating to at least \$5,000 in value.

See 18 U.S.C. §§ 1030(a)(5)(A)(iii), (e)(8), (g). Notably, the criminal component of this section requires that the Government prove *all of the same* elements as the civil claim, *see id.*, but again under the higher standard of proof of beyond a reasonable doubt.

b. Potential Civil and Criminal Remedies

The civil remedies are again the same as in the sections described above. See 18 U.S.C. § 1030(g). The potential criminal penalties and the classification of this offense depend on the circumstances of the infraction. The offense would be classified as a Class D felony, and a violator would be subject to a fine and/or up to 5 years of imprisonment, if the Government were to demonstrate that the violator *recklessly* caused the impairment of the integrity or availability of data, a program, a system, or information. See 18 U.S.C. §§ 1030(a)(5)(A)(ii), (c)(4)(B), 3559(a)(4). If, on the other hand, the Government cannot prove the recklessness requirement, and instead can only prove that a violator simply caused such impairment (regardless of his or her state of mind), then the offense becomes a Class A misdemeanor punishable by a fine and/or up to 1 year in prison. See *id.* §§ 1030(a)(5)(A)(iii), (c)(2)(A), 3559(a)(6).

4. Transmission of a Program that Causes Damage

Section 1030(a)(5)(A)(i) of the CFAA prohibits a person from knowingly causing the transmission of a program and thereby intentionally causing damage, without authorization, to a computer.

a. The Elements of the Claim/Crime

To state a civil claim under Section 1030(a)(5)(A)(i), a plaintiff must demonstrate that the defendant:

- (1) knowingly caused the transmission of a program, information, code, or command;
- (2) intentionally causing damage, *i.e.*, impairing the integrity or availability of data, a program, a system, or information, without authorization;

⁴ Sub-sections (ii) and (iii) of the CFAA differ slightly on this element, with the difference influencing the length of a possible prison sentence (and having no effect on a civil cause of action). Whereas sub-section (iii) simply requires that the conduct at issue have caused damage—*i.e.*, no specific scienter on the part of the violator need be shown—sub-section (ii) requires a showing that the violator *recklessly* caused damage. As is discussed below, a conviction under sub-section (iii) can lead to imprisonment of up to 1 year, whereas a conviction under sub-section (ii) can lead to imprisonment of up to 5 years.

- (3) to a protected computer; and
- (4) loss to 1 or more persons during any 1-year period aggregating to at least \$5,000 in value.

See 18 U.S.C. §§ 1030(a)(5)(A)(i), (e)(8), (g). The criminal component of this section requires that the Government prove *all of the same* elements as the civil claim, *see id.*, but again under the reasonable-doubt standard.

b. Potential Civil and Criminal Remedies

Again, no changes here with respect to civil remedies. See 18 U.S.C. § 1030(g). An offense under this section of the CFAA is classified as a Class C felony, and a violator would be subject to a fine and/or up to ten years of imprisonment. See 18 U.S.C. §§ 1030(c)(4)(A), 3559(a)(3).

5. Definitions of Damage and Loss

The CFAA defines “damage” as “any impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8). It defines “loss” as:

any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

Id. § 1030(e)(11).

B. THE WIRETAP ACT (as amended by the ECPA)

The Wiretap Act, *see* 18 U.S.C. §§ 2510 *et seq.*, prohibits the interception and disclosure of certain electronic communications. The Act prohibits several different types of activities and therefore could form the basis for several different causes of action or offenses. As with the other statutes discussed in this handout, the Wiretap Act may be enforced by criminal prosecution or by a private civil cause of action.

a. *The Elements of the Various Potential Claims/Crimes*

In order to state a civil claim under Section 2511(1)(a), a plaintiff must demonstrate that the defendant:

- (1) intentionally intercepted, endeavored to intercept, or procured another person to intercept or endeavor to intercept;
- (2) any wire, oral, or electronic communication.⁵

See 18 U.S.C. § 2511(1)(a). Each of the other potential claims under the Wiretap Act are similar in that they also require an interception. *See id.* § 2511(1)(c) (prohibiting the intentional disclosure of the contents of any communication where the person knows or has reason to know that the information was obtained through the interception of the communication); § 2511(1)(d) (prohibiting the intentional use of the contents of any communication where the person knows or has reason to know that the information was obtained through the interception of the communication). The criminal component of the Wiretap Act requires the same elements for each of these three potential violations, albeit with the higher standard of proof.

b. *Potential Civil and Criminal Remedies*

A court in a civil proceeding can award the plaintiff (1) preliminary and other equitable or declaratory relief; (2) the greater of (a) actual damages suffered by the plaintiff plus any profits made by the violator, or (b) statutory damages in the amount of \$100 a day for each day of violation or \$10,000, whichever is greater; (3) punitive damages; and (4) reasonable attorneys' fees. *See* 18 U.S.C. §§ 2520(b), (c)(2). A criminal violation of the Wiretap Act is a Class D felony and is punishable by a fine and/or up to 5 years in prison. *See id.* §§ 2511(4)(a), 3559(a)(4).

⁵ E-mails qualify as an electronic communication. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875 (9th Cir. 2002).

C. THE STORED COMMUNICATIONS ACT

The Stored Communications Act (SCA), *see* 18 U.S.C. §§ 2701 *et seq.*, prohibits the unlawful access to certain stored electronic communications. The SCA contains a single possible claim/offense. As with the other statutes discussed in this handout, the claim may be enforced by criminal prosecution or by a private civil cause of action.

a. The Elements of the Claim/Crime

To state a claim under Section 2701(a), the plaintiff must demonstrate that the defendant:

- (1) intentionally accessed without authorization or by exceeding an authorization;⁶
- (2) a facility through which an electronic communication service is provided; and
- (3) thereby obtained, altered or prevented authorized access to an electronic communication while it was in electronic storage.

See 18 U.S.C. § 2701(a). The statute defines an “electronic communication service” as any “service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15). The criminal component of this statute requires the Government to prove the same elements, *see id.*, albeit pursuant to a higher standard of proof.

The key component of the SCA is “electronic storage.” That term is defined in the statute as:

- (1) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; or
- (2) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

See 18 U.S.C. § 2510(17) (the statute uses the word “and” between the two elements but from the context it appears “or” was intended).

b. Potential Civil and Criminal Remedies

Potential civil remedies include: (1) preliminary and other equitable or declaratory relief; (2) the greater of (a) actual damages suffered by the plaintiff plus any profits made by the violator,

⁶ The SCA also speaks of authorization in another section of the statute, entitled “Exceptions.” That section provides that the SCA does not apply to conduct authorized (1) by the person or entity providing a wire or electronic communications service; or (2) by a user of that service with respect to a communication of or intended for that user. *See* 18 U.S.C. §§ 2701(c)(1), (2).

or (b) statutory damages of \$1,000; (3) punitive damages if the violation is found to be willful or intentional; and (4) reasonable attorneys' fees. *See* 18 U.S.C. §§ 2707(b), (c).

The potential criminal penalties and the classification of the offense under the SCA depend on the circumstances. Offenses under the SCA are classified as a Class D felony, and the violator would be subject to a fine and/or up to 5 years imprisonment, if the Government were to demonstrate that the offense was committed (1) for purposes of commercial advantage, malicious destruction or damage, or private financial gain; or (2) in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State. *See* 18 U.S.C. §§ 2701(b)(1), 3559(a)(4). In any other case, the offense is classified as a Class A misdemeanor, and the violator would be subject to a fine and/or a maximum term of imprisonment of 1 year. *See id.* §§ 2701(b)(2)(a), 3559(a)(6).

D. CAN-SPAM ACT

We have already seen how the federal CAN-SPAM Act imposes civil remedies for fraud in connection with electronic mail. But it also contains criminal penalties. It is a crime to knowingly (1) initiate the transmission, to a protected computer, of any commercial e-mail that includes sexually oriented material and (2) either—

- (a) fails to include in the subject heading SEXUALLY-EXPLICIT; or
- (b) displays the sexually oriented material to the recipient without his taking any affirmative steps to view it.

15 U.S.C. § 7704(d)(1); 16 C.F.R. § 316.4(a)(1). A criminal violation under this section is a Class D felony and is punishable by a fine and/or up to 5 years in prison. *See id.* 15 U.S.C. § 7704(d)(5), 18 U.S.C. § 3559(a)(4).

CAN-SPAM created other criminal violations relating to SPAM e-mails and practices. They can be found in 18 U.S.C. § 1037. I do not expect you to know the specifics of the statute, nor all the elements of the § 1037 violations, beyond what is already described in the casebook at pp. 1033-34.

E. TRUTH IN DOMAIN NAMES ACT

In 2003, Congress passed the Truth in Domain Names Act (TDNA), as part of the more comprehensive Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act (aka PROTECT Act).⁷ The TDNA contains, among other things, a section prohibiting misleading domain names, which provides that whoever

- (1) knowingly uses a misleading domain name on the Internet with the intent to deceive a person into viewing material constituting obscenity; or
- (2) knowingly uses a misleading domain name on the Internet with intent to deceive a minor into viewing material that is harmful to minors on the Internet,

shall be fined and/or imprisoned for not more than 2 years (for a violation of § 1, a Class E felony) or not more than 4 years (for a violation of § 2, a Class E felony). See 18 U.S.C. §§ 2252B(a), (b); 3559(a)(5).

The statute goes on to say that a domain name with words that indicate sexual content, such as “sex” or “porn,” is not misleading. *Id.* § 2252B(c). It then defines “material that is harmful to minors” and the word “sex.” *Id.* § 2252B(d), (e). The latter is fairly self-explanatory (think broader than President Clinton’s definition of the term). Here is how Congress defines “harmful to minors”:

any communication, consisting of nudity, sex, or excretion, that, taken as a whole and with reference to its context—

- (1) predominantly appeals to a prurient interest of minors;
- (2) is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and
- (3) lacks serious literary, artistic, political, or scientific value for minors.

⁷ Who comes up with these acronyms?

F. CRIMINAL COPYRIGHT INFRINGEMENT

The Copyright Act, *see* 17 U.S.C. § 506, provides for certain criminal penalties for willful infringements.

a. *The Elements of the Crime*

The Government must demonstrate that the defendant (1) willfully infringed a copyright and (2) either that the infringement was:

- (a) for purposes of commercial advantage or private financial gain;
- (b) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies of 1 or more copyrighted works, which have a total retail value of more than \$1,000; *or*
- (c) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution.

See 17 U.S.C. § 506(a)(1).

b. *Potential Criminal Remedies*

The criminal penalties for copyright infringement differ depending on which subsection of 506(a)(1) has been violated. A violation of subsection (a), *supra*, calls for a fine and/or a term of imprisonment with a maximum ranging from 1 year to 10 years, depending on whether it is the defendant's first offense under the statute, the number of copies made, and their retail value. *See* 18 U.S.C. § 2319(b). As such, the offense classification would range from a Class A misdemeanor to a Class C felony. *See* 18 U.S.C. §§ 3559(a)(3), (4), (6).

A violation of subsection (b) similarly calls for a fine and/or a term of imprisonment, with a maximum range also varying between 1 year and 6 years, again depending on whether it is the defendant's first offense, the number of copies made, and their retail value. *See* 18 U.S.C. § 2319(c). In this case, the offense classification would range from a Class A misdemeanor to a Class D felony. *See* 18 U.S.C. §§ 3559(a)(4)–(6).

Lastly, a violation of subsection (c) also calls for a fine and/or a term of imprisonment, with the maximum ranging from 3 years to 10 years, depending on whether the offense was committed for purposes of commercial advantage or private financial gain, and on whether it is the defendant's first offense under the statute. *See* 18 U.S.C. § 2319(d). The classification, then, would range between a Class E felony and a Class C felony. *See* 18 U.S.C. §§ 3559(a)(3)–(5).

G. THE IP PROTECTION AND COURT AMENDMENTS ACT

In 2004, Congress amended numerous statutes to increase protection for intellectual property, among other things. One of the most interesting provisions was a *sentencing enhancement* for crimes involving the false registration of domain names. *See* 18 U.S.C. § 3559(f).

The pertinent section provides that if a defendant is convicted of a felony offense (other than an offense for which an element is the false registration of a domain name)⁸ and the defendant

- (1) knowingly falsely registered a domain name; *and*
- (2) knowingly used that domain name in the course of the underlying offense,

then the maximum imprisonment otherwise provided by law for the underlying offense must be doubled or increased by 7 years, whichever is less. *See Id.* § 3559(f)(1). The statute goes on to define “falsely registers” as “registers in a manner that prevents the effective identification of or contact with the person who registers.” *Id.* § 3559(f)(2)(A).

⁸ As of this writing, there was no stand-alone false-registration crime on the books (cf. TDNA *supra*).