

Information Privacy—Statutory Claims Under the CFAA, SCA, and Wiretap Act

Prof. H. Tomás Gómez-Arostegui
Lewis & Clark Law School

A. THE COMPUTER FRAUD AND ABUSE ACT

The Computer Fraud and Abuse Act (CFAA), *see* 18 U.S.C. § 1030, prohibits a variety of 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. There are other potential claims available under § 1030, but the ones discussed below are of the kind most likely to be brought by individuals or businesses in the course of civil litigation.

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
- (3) that the conduct involved an interstate or foreign communication;³

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). Computers connected to the Internet and that are “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).

- 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), (a)(5)(B)(i), (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 of course 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 *id.* § 1030(g). The CFAA does not award the prevailing party attorneys' fees nor does it provide for punitive damages. The potential criminal penalties and the classification of this offense depend on the circumstances. 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 *Id.* §§ 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).

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 *id.* §§ 1030(a)(4), (a)(5)(B)(i), (g). The criminal component of this section requires the Government to prove the same elements, with the exceptions, again, that 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 *id.* § 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)(A)(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 *id.* §§ 1030(a)(5)(A)(iii), (a)(5)(B)(i), (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 *Id.* § 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

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.

that the violator *recklessly* caused the impairment of the integrity or availability of data, a program, a system, or information. *See id.* §§ 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;
- (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 id. §§ 1030(a)(5)(A)(i), (a)(5)(B)(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 id.* § 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 id.* §§ 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.” *Id.* § 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).

6. Limitation of Actions/Prosecutions Under the CFAA

Civil actions must be brought “within 2 years of the date of the act complained of or the date of the discovery of the damage.” *Id.* § 1030(g). The period of limitations for a criminal prosecution requires the indictment to be found or the information to be instituted “within five years next after such offense shall have been committed.” *Id.* § 3282(a).

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 id. §§ 2511(1)(a), 2520(a). Each of the other potential claims under the Wiretap Act are similar in that they also require an interception. *See id.* § 2511(1)(b)–(e). 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.

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

Federal courts, including those within the Ninth Circuit, have held that an “interception” of an electronic communication must be made during its transmission in order to implicate the Wiretap Act.

[T]here is only a narrow window during which an E-mail interception may occur—the seconds or milli-seconds before which a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee’s messages are automatically sent to the employee’s boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.

U.S. v. Steiger, 318 F.3d 1039, 1050 (11th Cir. 2003); *see also Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (“We therefore hold that for a website such as Konop’s to be ‘intercepted’ in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage.”); *Steve Jackson Games Inc. v. U.S. Secret Service*, 36 F.3d 457, 462 (5th Cir. 1994) (noting the “distinctions Congress intended to draw between communications being transmitted and communications in electronic storage”).⁶

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 id.* §§ 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).

c. Limitation of Actions/Prosecutions

A civil action must be brought within two years “after the date upon which the claimant first has a reasonable opportunity to discover the violation.” *Id.* § 2520(e). The limitations period for a criminal prosecution requires the indictment to be found or the information to be instituted within five years “after such offense shall have been committed.” *Id.* § 3282(a).

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

⁶ *See also Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 634-35 (E.D. Pa. 2001); *U.S. v. Simons*, 29 F. Supp. 2d 324, 329-30 (E.D. Va. 1998); *Wesley College v. Pitts*, 974 F. Supp. 375, 387 (D. Del. 1997).

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

- (1) intentionally accessed without authorization or by exceeding an authorization;⁷
- (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 id. § 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.” *Id.* § 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 id. § 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, 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 id.* §§ 2707(b), (c).

⁷ 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).

The potential criminal penalties and the classification of the offense under the SCA depend on the circumstances. Offenses 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 id.* §§ 2701(b)(1), 3559(a)(4). In any other case, it is 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).

c. Limitation of Actions/Prosecutions

A civil action must be brought within two years “after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.” *Id.* § 2707(f). A criminal prosecution must be brought within five years “after such offense shall have been committed.” *Id.* § 3282(a).