Chapter 3
Other Network Crime Statutes

A. Unlawful Access to Stored Communications: 18 U.S.C. § 2701

Section 2701 focuses on protecting email and voicemail from unauthorized access. *See* H.R. Rep. No. 647, 99th Cong., 2d Sess., at 63 (1986). At heart, section 2701 is designed to protect the confidentiality, integrity, and availability of such communications stored by providers of electronic communication service pending the messages' ultimate delivery to their intended recipients.

Summary

1. Intentional access
2. without or in excess of authorization
3. a facility that provided an electronic communication service
4. obtained, altered, or prevented authorized access to a communication in electronic storage
5. (felonies only) for commercial advantage, malicious destruction or damage, private commercial gain, or in furtherance of a criminal or tortious act

A charge under section 2701 has four essential elements. A felony conviction requires proof of one additional element.

Title 18, United States Code, Section 2701(a) provides:

Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

1. Intentional Access

The *mens rea* element of a section 2701 violation is that the defendant's unauthorized access (or access in excess of authorization) was intentional. Although no court has analyzed the *mens rea* requirement for this section,

courts have addressed the *mens rea* requirement for similar language in 18 U.S.C. § 1030. *See United States v. Sablan*, 92 F.3d 865, 867-68 (9th Cir. 1996); *United States v. Morris*, 928 F.2d 504, 508-09 (2d Cir. 1991). *Sablan* analyzed the wording, structure, and purpose of what was then § 1030(a)(5)(A) and concluded that the "intentionally" language modified only the "accesses without authorization" portion of that statute. *Sablan*, 92 F.3d at 868. The same reasoning applies to section 2701. Therefore, the government must prove that a defendant's access without authorization (or access in excess of authorization) was intentional.

The term "access" is not defined in this statute, but the term is discussed beginning on page 32. In a typical criminal case, in which a defendant will have logged on to a system and obtained, altered, or deleted email or voicemail, there will be no question that the defendant has accessed a facility.

2. Without or In Excess of Authorization

The second element of section 2701 requires proof that the defendant either was not authorized to access the facility or the defendant exceeded authorized access. This element mirrors the "without authorization" and "exceeds authorized access" language of 18 U.S.C. § 1030. For the discussion of the meaning of these terms, please see page 4.

3. Facility Through Which an Electronic Communication Service Is Provided

The third element of a section 2701 violation is that the defendant accessed a facility through which an electronic communication service (ECS) was provided. An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). In other words, an ECS is a facility that others use to transmit communications to third parties. Section 2701 incorporates that definition. *See* 18 U.S.C. § 2711(1). For example, logging on to an email server will satisfy this element. "[T]elephone companies and electronic mail companies" generally act as providers of electronic communication services. *See* S. Rep. No. 541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568. A provider of email accounts over the Internet is a provider of ECS, *see FTC v. Netscape Communications Corp.*, 196 F.R.D. 559, 560 (N.D. Cal. 2000), as is the host of an electronic bulletin board. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 879-80 (9th Cir. 2002). Thus, computers which provide such services are facilities through which an ECS is provided. *See Snow v. DirectTV*, 450 F.3d 1314 (11th Cir.

2006) (upholding a dismissal for failure to state a claim, where defendants used computers to access a website generally available to the public).

However, not every computer or device connected to a communication system is a facility through which an ECS is provided: a computer or device belonging to an end-user of ECS is not such a facility. For example, the Eleventh Circuit has held that hacking into a home computer does not by itself implicate section 2701, because a home computer does not provide an ECS to others. *See United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003). Similarly, the court in *State Wide Photocopy Corp. v. Tokai Fin. Services, Inc.*, 909 F. Supp. 137, 145 (S.D.N.Y. 1995), rejected the assertion that a business's computers and fax machines constituted facilities through which an ECS is provided. Courts have also rejected the notion that maintaining a website or merely utilizing Internet access constitutes providing an ECS. *See Dyer v. Northwest Airlines Corp.*, 334 F. Supp. 2d 1196, 1999 (D.N.D. 2004) (holding that airline selling travel services over the Internet is not a provider of ECS); *Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001) (holding that Amazon.com is not a provider of ECS).

4. Affected Authorized Access to a Communication In Electronic Storage

The fourth element of a section 2701 violation is that the defendant obtained, altered, or prevented authorized access to a wire or electronic communication while it was in "electronic storage." This element has three components. The first component, that the defendant "obtained, altered, or prevented authorized access to," means that a defendant must acquire a stored communication, modify a stored communication, or prevent proper access to a stored communication.

The Ninth Circuit, when distinguishing access under section 2701 from an interception under the Wiretap Act, misinterpreted this component. In *United States v. Smith*, 155 F.3d 1051 (9th Cir. 1998), the Ninth Circuit stated that "[t]he word 'intercept' entails *actually* acquiring the contents of a communication, whereas the word 'access' merely involves *being in position* to acquire the contents of a communication." *Smith*, 155 F.3d at 1058 (emphasis in original). It then opined that one might violate section 2701 by using a purloined password to log on to a voicemail system without ever obtaining the contents of any voicemail. *See id.*

This voicemail comment and definition of "access" ("obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage") indicate that the Ninth Circuit misread this component. It read "obtained," "altered," or "prevented authorized" as modifying "access to a wire or electronic communication," rather than reading "obtained," "altered," or "prevented authorized access to" as modifying "a wire or electronic communication." Thus, in the Ninth Circuit's voicemail example, the defendant will have obtained access to a wire communication, because the defendant will have been in a position to access the wire communication. However, even with the Ninth Circuit's definition of "access," this parsing of section 2701 does not make sense. In particular, it does not make sense for "altered" to modify "access to a wire or electronic communication." Instead, "altered" properly modifies "communication" and simply means "changed the communication." Because *Smith* misread section 2701, its definition of "access" should carry little weight.

The second component, that the conduct involved a "wire or electronic communication," needs little further explanation. Essentially, a wire communication is defined as a communication containing the human voice that is transmitted in part by wire or other similar method. *See* 18 U.S.C. § 2510(1), (18). In addition, "electronic communication" is defined broadly in 18 U.S.C. § 2510(12) and includes most electric or electronic signals that are not wire communications. For example, voicemail is a wire communication, and email and other typical Internet communications that do not contain the human voice are electronic communications.

The final component of this element is that the communication was in "electronic storage." The term "electronic storage" has a narrow, statutorily defined meaning. It does *not* simply mean storage of information by electronic means. Instead, "electronic storage" is "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). As traditionally understood by the government, "electronic storage" refers only to temporary storage, made in the course of transmission, by a provider of electronic communications service, and to backups of such intermediate communications. If the communication has been received by a recipient's service provider but has not yet been accessed by the recipient, it is in "electronic storage." For example, a copy of an email

or voicemail is in "electronic storage" only if it is at an intermediate point in its transmission and has not yet been retrieved by its intended recipient (e.g. "unopened email"). When the recipient retrieves the email or 18 U.S.C. §, however, the communication reaches its final destination. If the recipient chooses to retain a copy of the communication on the service provider's system, the retained copy is no longer in "electronic storage" because it is no longer in "temporary, intermediate storage ... incidental to ... electronic transmission," and neither is it a backup of such a communication. *See Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 635-36 (E.D. Pa. 2001), *aff'd in part* 352 F.3d 107, 114 (3d Cir. 2004) (upholding district court's ruling on other grounds). Instead, it is treated like any other material stored by a user under provisions governing remote computing services. *See* H.R. Rep. No. 647, 99th Cong., 2d Sess., at 65 (1986) (stating that when a recipient has retrieved an email message and chooses to leave it in storage with the service provider, the email is protected under a provision of 18 U.S.C. § 2702 applicable to remote computing services).

This long-standing narrow interpretation of "electronic storage" was rejected by the Ninth Circuit in *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004). In *Theofel*, the Ninth Circuit held that email messages were in electronic storage regardless of whether they had been previously accessed. Although the Ninth Circuit did not dispute that previously accessed email was not in temporary, intermediate storage within the meaning of § 2510(17)(A), it insisted that previously accessed email fell within the scope of the "backup" portion of the definition of "electronic storage." *See id.* at 1075. Under *Theofel*, essentially all stored wire or electronic communications are in "electronic storage."

If *Theofel*'s broad interpretation of "electronic storage" were correct, prosecutions under section 2701 would be substantially less difficult, as it can be hard to prove that communications fall within the traditional narrow interpretation of "electronic storage." However, CCIPS continues to question whether *Theofel* was correctly decided, since little reason exists for treating old email differently than other material a user may choose to store on a network. Any prosecutor considering a prosecution under section 2701 that relies on *Theofel* is urged to contact CCIPS for consultation.

5. Purpose

Felony charges require proof of one additional element: that the defendant acted "for purposes of commercial advantage, malicious destruction or damage,

or private commercial gain, or in furtherance of any criminal or tortious act." 18 U.S.C. § 2701(b)(1).[1] This element was added by the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002), and it applies to conduct after January 23, 2003. All first-time violations of section 2701 prior to that date are misdemeanors. Such language is also used in the Wiretap Act, as an exception to when a party may consent to interception of their communications. *See* 18 U.S.C. § 2511(2)(d). In the Wiretap Act context, one appellate court has stated that this language is operative when a prohibited purpose is either the subject's primary motivation or a determinative factor in the subject's motivation. *See United States v. Cassiere*, 4 F.3d 1006, 1021 (1st Cir. 1993). Naturally, the "in furtherance of any criminal or tortious act" language means an act other than the unlawful access to stored communications itself. *See Boddie v. American Broadcasting Co.*, 731 F.2d 333, 339 (6th Cir. 1984).

6. Exceptions

Section 2701(c) provides three statutory exceptions to a violation. First, the section does not apply to "the person or entity providing a wire or electronic communication service." 18 U.S.C. § 2701(c)(1). Thus, unlike in the Wiretap Act context, service providers cannot violate § 2701, regardless of their motives in accessing stored communications. *See United States v. Councilman*, 418 F.3d 67, 81-82 (1st Cir. 2004) (en banc). Second, the section does not apply to conduct authorized by a user "with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c)(2). *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 880 (9th Cir. 2002) (interpreting "user" narrowly to exclude someone who was properly authorized to access an electronic bulletin board, but who had not actually done so). Third, section 2701 does not apply to conduct authorized by other sections of the Act or the Wiretap Act. *See* 18 U.S.C. § 2701(c)(3). Although no court has yet addressed the role of these exceptions in a criminal prosecution, they should be viewed as creating affirmative defenses rather than statutory elements. *See generally United States v. Kloess*, 251 F.3d 941, 944-46 (11th Cir. 2001) (discussing distinctions between elements of a crime and affirmative defenses created by statutory exceptions).

[1] Similar language appears in the CFAA, 18 U.S.C. § 1030(c)(2)(B), to enhance the penalty for a violation of § 1030(a)(2), which criminalizes accessing a computer without authorization or in excess of authorization.

7. Penalties

The penalties for unlawful access to stored communications are divided into three categories. For first-time violations not committed for a specified improper purpose (that is, not committed "for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act"), the maximum penalty is one year imprisonment and a $100,000 fine. *See* 18 U.S.C. §§ 2701(b)(2)(A), 3571(b)(5). For repeat violations not committed for an improper purpose, or for first-time violations committed for an improper purpose, the maximum penalty is five years' imprisonment and a $250,000 fine. *See* 18 U.S.C. §§ 2701(b)(1)(A), (b)(2)(B), 3571(b)(3). For repeat violations committed for an improper purpose, the maximum penalty is ten years' imprisonment and a $250,000 fine. *See* 18 U.S.C. §§ 2701(b)(1)(B), 3571(b)(3).

8. Historical Notes

The Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712, sets forth a system of statutory privacy rights for customers and subscribers of computer network service providers. This system has three main substantive components that serve to protect and regulate the privacy interests of network users with respect to the world at large, network service providers, and the government. The first component of this system is a criminal prohibition. Under section 2701 of the SCA, anyone who obtains, alters, or prevents authorized access to certain stored communications is subject to criminal penalties. Neither of the other substantive components of the SCA is criminal: section 2702 regulates voluntary disclosure by network service providers of customer communications and records, and section 2703 creates a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications and related records.

Since its enactment in 1986, there have been very few prosecutions under section 2701. There are at least three reasons for this lack. First, prior to the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002), all first-time violations of this section were misdemeanors. That Act, however, changed the maximum penalty for first-time violations to five years when the offense is committed "for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State." 18 U.S.C. § 2701(b)(1). Second, one element of

prosecutions can be difficult to prove: that the defendant obtained, altered, or prevented authorized access to communications in "electronic storage," a term which is narrowly defined in 18 U.S.C. § 2510(17) and which has traditionally been interpreted to include only communications which have not yet been accessed by their intended recipient. Third, many violations of section 2701 also involve conduct that violates 18 U.S.C. § 1030. Because prosecutions under section 1030 do not involve proof that a communication is in "electronic storage," it will often be easier for the government to prove a violation of section 1030 than section 2701.

B. Identity Theft: 18 U.S.C. § 1028(a)(7)

Network intrusions can compromise the privacy of individuals if data about them or their transactions resides on the victim network. These cases should also be analyzed for potential violations of identity theft statutes. For a more detailed treatment of identity theft, see U.S. Department of Justice, *Identity Theft and Social Security Fraud* (Office of Legal Education 2004).

Several federal laws apply to identity theft, including 18 U.S.C. section 1028. That section criminalizes eight types of conduct involving fraudulent identification documents or the unlawful use of identification information. Section 1028(a)(7), enacted as part of the Identity Theft and Assumption Deterrence Act of 1998, and amended in 2004 by the Identity Theft Penalty Enhancement Act, will apply to some network crime cases.

Title 18, United States Code, Section 1028(a)(7) provides:

> *Whoever, in a circumstance described in subsection (c) of this section–*
>
> *(7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable*
>
> *shall be punished as provided in subsection (b) of this section.*

The term "means of identification" is defined as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual." 18 U.S.C. § 1028(d)(7). It covers several specific examples, such as name, social security number, date of birth, government issued driver's license and other numbers; unique biometric data, such as fingerprints, voice print, retina or iris image, or other unique physical

representation; unique electronic identification number, address, or routing code; and telecommunication identifying information or access device. *Id.*

Section 1028(a)(7) requires a predicate offense, much like 18 U.S.C. § 1028A (discussed below). Unlike section 1028A, however, the scope of section 1028(a)(7) is much broader. Section 1028A depends solely on certain enumerated federal felonies. *See* 18 U.S.C. § 1028A(a)(1). Section 1028(a)(7), on the other hand, may be based on *any* federal violation (felony or misdemeanor), as well as any local or state felony. *See* 18 U.S.C. § 1028(a)(7).

C. Aggravated Identity Theft: 18 U.S.C. § 1028A

The Identity Theft Penalty Enhancement Act, which took effect July 15, 2004, established a new offense of aggravated identity theft. Section 1028A adds an additional two-year term of imprisonment in cases where a defendant "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person" during and in relation to any felony violation of certain enumerated federal offenses, including 18 U.S.C. §§ 1028 (but not 1028(a)(7)), 1029, 1030, 1037, and 1343. *See* 18 U.S.C. § 1028A(a)(1). In cases of terrorism-related aggravated identity theft, including that related to section 1030(a)(1), that section imposes an additional five-year term of imprisonment. 18 U.S.C. § 1028A(a)(2). In most cases, the additional terms of imprisonment will run consecutively, not concurrently. 18 U.S.C. § 1028A(b).

For questions regarding the application of this provision, please contact the Fraud Section of the Criminal Division of the Department of Justice at (202) 514-7023.

D. Access Device Fraud: 18 U.S.C. § 1029

Ten separate activities relating to access devices are criminalized in 18 U.S.C. § 1029. The term "access device" is broadly defined to mean "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)."

18 U.S.C. § 1029(e)(1). Access devices related to network crimes might include passwords, electronic banking account numbers, and credit card numbers.

Generally speaking, section 1029 prohibits the production, use, possession, or trafficking of unauthorized or counterfeit access devices. Prosecutors should note the difference between "unauthorized" and "counterfeit" devices because certain key sections of the statute are based on these two terms. *See* 18 U.S.C. §§ 1029(e)(2) & (3). Section 1029 also covers activities related to certain tools and instruments that are used to obtain unauthorized use of telecommunications services. *See* 18 U.S.C. §§ 1029(a)(7)-(9).

Charges under section 1029 would be useful in many types of "phishing" cases, where a defendant uses fraudulent emails to obtain various types of passwords and account numbers, and "carding" cases, where a defendant purchases, sells, or transfers stolen bank account, credit card, or debit card information. Penalties for violations of section 1029 range from a maximum of 10 or 15 years' imprisonment depending on the subsection violated. *See* 18 U.S.C. § 1029(c)(1)(A). Second and later offenses are subject to 20 years' imprisonment. *See* 18 U.S.C. § 1029(c)(1)(B). Forfeiture is also available in many cases. *See* 18 U.S.C. §§ 1029(c)(1)(C), (c)(2).

For more information about section 1029, please contact the Fraud Section of the Criminal Division of the Department of Justice at (202) 514-7023. For specific information about subsections (7), (8), or (9), please contact CCIPS at (202) 514-1026.

E. CAN-SPAM Act: 18 U.S.C. § 1037

The CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003), which became effective on January 1, 2004, provides a means for prosecuting those responsible for sending large amounts of unsolicited commercial email (a.k.a. "spam"). Although civil and regulatory provisions are the primary mechanism by which the CAN-SPAM Act's provisions are enforced, it also created several new criminal offenses at 18 U.S.C. § 1037. These offenses are intended to address more egregious violations of the CAN-SPAM Act, particularly where the perpetrator has taken significant steps to hide his or her identity, or the source of the spam, from recipients, ISPs, or law enforcement agencies.

In addition to section 1037, the CAN-SPAM Act contains another criminal provision, codified at 15 U.S.C. § 7704(d), which prohibits sending sexually explicit email that does not contain a label or marking designating it as sexually explicit. A knowing violation of this section is punishable by a fine, imprisonment for not more than five years, or both. For questions regarding the application of § 7704(d), please contact the Child Exploitation and Obscenity Section of the Criminal Division of the Department of Justice at (202) 514-5780.

Title 18, United States Code, Section 1037(a) provides:

Whoever, in or affecting interstate or foreign commerce, knowingly–

(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,

(2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,

(3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,

(4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or

(5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses, or conspires to do so, shall be punished as provided in subsection (b).

1. Commercial Electronic Mail Messages

Section 1037 only criminalizes conduct involving "commercial electronic mail messages":

> (A) In general. The term "commercial electronic mail message" means any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial

> product or service (including content on an Internet website operated for a commercial purpose).
>
> (B) Transactional or relationship messages. The term "commercial electronic mail message" does not include a transactional or relationship message.

15 U.S.C. § 7702(2).

2. Materially

Sections 1037(a)(3) and (a)(4) require proof that certain information was "materially" falsified:

> For purposes of paragraphs (3) and (4) of subsection (a), header information or registration information is materially falsified if it is altered or concealed in a manner that would impair the ability of a recipient of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation.

18 U.S.C. § 1037(d)(2).

3. Multiple

Section 1037 only criminalizes conduct involving "multiple" commercial email messages:

> The term "multiple" means more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a one-year period.

18 U.S.C. § 1037(d)(3).

4. Penalties

A violation of section 1037 is a felony punishable by a fine, imprisonment for not more than five years, or both, if:

> (A) committed in furtherance of any felony under the laws of the U.S. or of any State; or

(B) the defendant has previously been convicted under § 1037, § 1030, or the law of any State for conduct involving the transmission of spam or unauthorized access to a computer system.

18 U.S.C. § 1037(b)(1).

A violation of section 1037 is a felony punishable by a fine, imprisonment for not more than three years, or both, if:

- committed in violation of § 1037(a)(1)
- committed in violation of § 1037(a)(4), and it involved 20 or more falsely registered email accounts, or 10 or more falsely registered domains
- the volume of email messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any one-year period
- the offense caused an aggregate loss of $5,000 or more to one or more persons during any one-year period
- any individual committing the offense obtained anything of value aggregating $5,000 or more during any one-year period; or
- the defendant undertook the offense with three or more persons and occupied an organizer or leadership position

18 U.S.C. § 1037(b)(2)(A)-(F).

All other violations of section 1037 are misdemeanors, punishable by a fine, imprisonment for not more than one year, or both. 18 U.S.C. § 1037(b)(3).

Section 1037 also contains specific provisions relating to forfeiture. 18 U.S.C. § 1037(c). For more information about forfeitures, please contact the Asset Forfeiture and Money Laundering Section of the Criminal Division of the Department of Justice at (202) 514-1263.

F. Wire Fraud: 18 U.S.C. § 1343

One particularly powerful and commonly applicable charge to consider is wire fraud. 18 U.S.C. § 1343. The United States Attorneys' Manual provides extensive guidance regarding wire fraud charges, *see* USAM § 9-43.000, as does the manual *Identity Theft and Social Security Fraud* (2004).

Title 18, United States Code, Section 1343 provides:

> *Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits, or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.*

1. Application to network crimes

Courts have recognized a variety of means of communications as falling under the wire fraud statute, including facsimile, telex, modem, and Internet transmissions. *See, e.g., United States v. Pirello*, 255 F.3d 728 (9th Cir. 2001) (affirming sentence of defendant who used the Internet to commit wire fraud).

Sections 1343 and 1030(a)(4) overlap to a degree in that both require fraudulent intent. Section 1343, however, carries significantly higher penalties. *Compare* 18 U.S.C. § 1343 (20 years' imprisonment; 30 years' imprisonment for fraud affecting financial institutions) *with* 18 U.S.C. § 1030(c)(3) (5 years' imprisonment for initial § 1030(a)(4) violation; 10 years for later violations). Section 1343 is also a predicate for RICO and money laundering charges, unlike section 1030 (with the exception of terrorism related violations of § 1030(a)(1) and 1030(a)(5)(A)(i)). For the full list of RICO predicate offenses, see 18 U.S.C. § 1961.

2. Penalties

Violations of this section are felonies, punishable by a fine, imprisonment for not more than 20 years, or both. 18 U.S.C. § 1343. If the violation affects a financial institution, the maximum penalty rises to a fine of up to $1,000,000, imprisonment for not more than 30 years, or both. *Id.*

G. Communication Interference: 18 U.S.C. § 1362

Where a compromised computer is owned or used by the United States for communications purposes, 18 U.S.C. § 1362 may provide an alternative or additional charge.

Title 18, United States Code, Section 1362 provides:

> *Whoever willfully or maliciously injures or destroys any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States, whether constructed or in process of construction, or willfully or maliciously interferes in any way with the working or use of any such line, or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system, or attempts or conspires to do such an act, shall be fined under this title or imprisoned not more than ten years, or both.*

1. Application to Network Crimes

Section 1362 applies to "any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States." 18 U.S.C. § 1362. The list of covered communications systems could include, for example, those used to provide electronic mail services.

Section 1362 is particularly useful in cases where the intrusion into a U.S. Government system would be a misdemeanor under § 1030 (e.g., first time violations of § 1030(a)(2)(B), (a)(3), (a)(5)(A)(iii), or (a)(6)(B)), but could be charged as a ten-year felony under § 1362.

2. Penalties

A violation of this section is a felony punishable by a fine, imprisonment for not more than 10 years, or both. 18 U.S.C. § 1362.