BINGHAM

LEGAL INSIGHT. BUSINESS INSTINCT.

Computer Crimes:

A Handbook of Civil and Criminal Issues For In-House Counsel

Table of Contents

TABLE OF CONTENTS.....1

ABOUT BINGHAM MCCUTCHEN.....2

INTRODUCTION.....3

SUMMARY OF TYPES OF CASES.....4

SUMMARY OF STATUTES.....7

The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522.....8

The Stored Communications Act, 18 U.S.C. §§ 2701-2712.....12

The Computer Fraud and Abuse Act, 18 U.S.C. § 1030.....16

California's Comprehensive Data Access and Fraud Act (Cal. Penal Code Section 502).....22

Laws Requiring Data Security and Breach Notification.....25

Other Computer Crime Related Laws.....26

AUTHOR CONTACTS.....28

About Bingham McCutchen

Bingham's market-leading practices are focused on global financial services firms and Fortune 100 companies. We have 1,000 lawyers in 14 offices in the U.S., Europe and Asia, including New York, London, Frankfurt, Tokyo, Hong Kong and Beijing. We are recognized leaders in our fields, and our work has been honored by *Chambers USA*, *Chambers UK*, *Chambers Asia*, *Best Lawyers in America*, *International Who's Who of Business Lawyers*, *PLC Cross-Border Handbook*, *Expert Guides* and other industry-rating publications. Our lawyers work in integrated teams across disciplines, ensuring that clients always have the right lawyers addressing their issues.

We regularly advise clients in civil and criminal computer crime matters. Among our lawyers are former government attorneys who prosecuted such cases and in-house counsel who have handled such cases. We pride ourselves on crisis management and a strategic approach that takes into account the relevant business issues.

Our practices include:

Litigation

- Antitrust and Trade Regulation
- Appellate
- Entertainment, Media and Communications
- Environmental, Land Use and Natural Resources
- Intellectual Property
- Labor and Employment
- Real Estate, Project Finance and Construction Litigation
- Securities and Financial Institutions Litigation
- White Collar Defense and Investigations

Financial Services

- Banking and Leveraged Finance
- Broker-Dealer
- Financial Restructuring
- Institutional Finance
- Investment Management
- Structured Transactions

Corporate

- Corporate, M&A and Securities
- Energy and Project Finance
- Government Affairs
- Private Equity
- Real Estate
- Tax and Employee Benefits
- Telecommunications, Media and Technology

Industry Groups

- Insurance
- Healthcare
- Life Sciences
- Privacy & Security

BINGHAM OFFICE LOCATIONS

- Beijing
- Boston
- Hartford
- Hong Kong
- Frankfurt
- London
- Los Angeles
- New York
- Orange County
- San Francisco
- Santa Monica
- Silicon Valley
- Tokyo
- Washington, D.C.

Introduction

Computer crimes, loosely defined, refer to the patchwork of federal and state statutes that prohibit certain conduct related to computers. In some instances, liability may be imposed for unauthorized access to computer systems and damage done to those systems. In other instances, liability may be imposed for accessing communications stored or in transit. Many of these statutes allow for both criminal and civil liability and provide for statutory damages, punitive damages, and awards of attorneys' fees.

As reliance on computers, mobile devices, and other electronic gadgets has mushroomed in recent years, computer crimes have increased dramatically. A segment on a Sixty Minutes broadcast titled "Cyber War: Sabotaging the System" reported that the United States probably lost the digital equivalent of the Library of Congress in 2007 when an unknown foreign power accessed systems operated by the Department of Defense, the Department of State, the Department of Commerce, and probably the Department of Energy and NASA. That same story reported that in 2008 someone was able to get past the firewalls and encryption devices of the CENTCOM network, the command overseeing the wars in Iraq and Afghanistan, and monitor that network. It is thought that this access was gained by leaving thumbnail drives (USB memory sticks) with malicious code on them lying around places where U.S. military personnel were likely to pick them up.

The examples in the private sector are also alarming. The 60 Minutes broadcast quoted Sean Henry, an assistant director of the FBI in charge of the Bureau's cyber division as stating "there are thousands of attempted attacks every day, tens of thousands of attacks." Henry told Sixty Minutes in late 2009 that criminals had used the Internet to steal more than $100 million from U.S. banks during that year. Henry reportedly had seen attacks where $10 million had been lost in one 24-hour period. Most states have laws that impose requirements to notify consumers when data is acquired by unauthorized persons and many state laws, as well as federal regulations, require reasonable safeguarding of consumer information, which includes, in some instances, the obligation to develop and implement internal data security policies and procedures, which require, inter alia, training of employees and due diligence in the selection of vendors who have access to customer information. Thus, in addition to investigating the crime itself, companies are often required to engage in costly notice processes and may face regulatory inquiry or civil suits stemming from such crimes.

Civil litigation involving alleged violations of computer crimes laws is also on the rise. In many instances, the allegations do not relate to the core criminal conduct discussed above, but instead involve companies' marketing practices, responses to government inquiries, or other conduct. It is not uncommon for companies to find themselves on both sides of civil computer crime litigation, leveraging the statutes offensively to protect their customers and their brand, as well as defending against claims brought against them. A significant challenge in such litigation is the fact that most of the applicable statutes were drafted many years before the development of current technology, and thus issues of interpretation exist.

This handbook is designed as a resource to assist in-house counsel in spotting computer crime issues and better understanding the applicable statutes. This handbook is not legal advice and is not comprehensive; every matter must be analyzed based on its unique facts. The summary is organized in two parts. The first part summarizes the types of cases that have been filed under the above statutes, focusing primarily on use of the statutes in civil litigation. The second part is designed as a quick reference guide to the relevant statutes, and outlines prohibited conduct and available damages with reference to case law interpreting the statutes.

Summary of Types of Cases

BACKGROUND

Computer crimes statutes are routinely criticized for failing to address evolving technology. For example, Congress passed the Electronic Communications Privacy Act (ECPA) in 1986. The Ninth Circuit has commented that a 1986 law is ill equipped to address modern technology: "The ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication . . . . Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002). Moreover, existing law is detailed and overlapping. Courts, for example, have called the intersection between the ECPA and the Stored Communications Act (SCA) "a complex, often convoluted, area of the law." *United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir.1998). It is thus often difficult to understand what laws apply to which technology and under what circumstances.

TYPES OF CLAIMS

The following section summarizes some of the types of claims that have been brought under computer crimes statutes. This summary is not meant to be exhaustive, but rather is meant to provide a framework for understanding generally some of the types of actions brought under some of the more commonly used statutes.

1. Business Protecting Customers

Companies have used computer crime statues to protect their customers. For example, in 1998, America Online succeeded on summary judgment in a claim that LCGM, a company alleged to have sent spam emails for pornographic web sites to AOL users, violated the Computer Fraud and Abuse Act (CFAA). *American Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D. Va. 1998). The Court held that LCGM violated at least two sections of the CFAA by intentionally accessing AOL's computers without authorization to acquire AOL user's email addresses using extractor software programs in violation of AOL's terms of service. Similarly, Facebook filed suit against a number of businesses and individuals for alleged theft and misuse of the usernames and passwords of Facebook users to allegedly gain access to Facebook's network and send unsolicited commercial messages to Facebook users. *See Facebook, Inc. v. Jeremi Fisher, et al.*, No. CV09-05842 (Dec. 14, 2009). That lawsuit alleged violations of the CFAA and California's Comprehensive Data Access and Fraud Act, Penal Code Section 502 (Section 502).

2. Customer Against Business

It is also common for customers to bring lawsuits, often as class actions, based on alleged unauthorized access and use of customer information. An action was filed against Quantcast and other defendants in *Edward Valdez v. Quantcast et al.,* No. CV 10-05484 (Jul. 23, 2010) for alleged violations of the CFAA and Section 502 resulting from the alleged use of flash cookies on users' computers that allegedly circumvented users' controls for managing web privacy and security. Similarly, a class action was filed against Facebook based on Facebook's "Instant Personalization" tool, a plug-in that allows third party websites to access users' personal information when users click on third party websites. *See Derrick Rose v. Facebook, Inc.*, No. CV-00232 (D.C. R.I. May 21, 2010). The complaint alleged that Facebook violated the SCA because the

Instant Personalization social networking tool exceeded authorization of users in accessing users' stored electronic communications. Apple has also faced lawsuits by iPhone and iPad owners under the ECPA, the CFAA, and other statutes for allegedly sending personal information to advertisers without consent of the users. *See Lalo v. Apple Inc.*, No. CV-10-5878 (N.D. Cal. Dec. 23, 2010). Recently there has been a slew of lawsuits against smartphone manufacturers and mobile network operators that use software tools, alleging that the software logs user information and transmits it without consent of the user.

3. Competitor Against Competitor

Competitors also may bring claims against other competitors. For example, Register.com obtained a preliminary injunction barring its competitor, Verio, Inc., from using automated software programs to access and collect Register.com's customer contact information contained in a public Internet domain registrant database. *Register.com v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000). In another case, Facebook filed suit against Power Ventures, Inc. (a website that attempted to aggregate different social networks into a single interface) for allegedly inducing visitors to surrender their Facebook usernames and passwords so defendants could access Facebook servers without authorization and use such information for commercial gain. *See Facebook, Inc. v. Power Ventures, et al.*, 2011 WL 3291750, at *11 (N.D. Cal. July 20, 2010). Facebook recently secured summary judgment for violations of the CFAA and Section 502. *See* Dkt. 275 (Feb. 16, 2012).

4. Employee Against Employer

Employees may also allege civil violations against employers for unauthorized access to the employee's accounts or information. For example, in *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 900 (9th Cir. 2008) (Certiorari granted on 4th Amendment claim only) an employee police officer filed suit alleging violations of the SCA by the employer police department for accessing his text messages sent on a department issued mobile phone where the messages themselves were not stored on department servers. In another case, *Pietrylo v. Hillstone Restaurant Group*, a jury found violations of the SCA where an employee of a Houston restaurant created a private, password protected, chat group on MySpace to discuss work issues and the employer obtained the password from an employee and accessed the private discussion group. Case No. cv-05754 (D.C. N.J. Sep. 25, 2009).

5. Employer Against Employee

Employers may also make claims against current or former employees for unauthorized access to computer systems or interception of communications. A common example is the disgruntled employee who accesses the email accounts of other employees or accesses computer files or data to which the employee does not have clearance or a need to know. These claims often arise in connection with employment claims (e.g. harassment), or in connection with theft of data. A report on a collaboration between Verizon and the Secret Service confirmed 141 data breach cases in 2009 that resulted in 143 million compromised records. That report demonstrated a much higher number of inside breaches than shown through previous reports, with 48% of breaches originating from inside a business or organization. Recent examples include a TD Ameritrade employee who sold customer information to stock spammers, a former T-Mobile employee who admitted selling large volumes of customer data to marketers, and a former Cisco employee who used a Cisco employee's password to gain access to the computer system to download proprietary and copyrighted software.

6. Government Prosecution

The government can also prosecute companies and individuals for violations of computer crime laws. For example, David Kernell was convicted by a federal jury in Knoxville, Tennessee on August 30, 2010 for intentionally accessing without authorization the email account of former Alaska governor Sarah Palin. After answering a series of security questions that allowed him to reset the password and gain access, Kernell read the contents of the account and made screenshots of the email directory and content, and subsequently posted the screenshots and new password to a public website. Kernell was sentenced to one year and a day in custody.

7. Subpoena Responses

Computer crimes statutes may also prohibit disclosures in response to subpoenas. Facebook, Myspace and Media Temple, for example, were served with third-party civil subpoenas requesting the contents of private messages sent between users and postings on the social networking cites. The Court quashed the subpoenas on the grounds that the communications were protected by the SCA and the government needed a search warrant to obtain the information. *See Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010). Similarly, in *Barnes v. CUS Nashville*, a plaintiff alleged she was encouraged by employees of Coyote Ugly Saloon to climb onto the bar to take photos, and when she did she slipped and fell. The defendant served Facebook with a civil subpoena for the plaintiff's Facebook information, including photos of plaintiff and her friends dancing on the bar. The magistrate judge quashed the subpoena finding the Facebook information protected by the SCA, and instead proposed creation of a Facebook account for an in camera review of the photographs and related comments. *See* WL 2196591 (M.D. Tenn. May 27, 2010). Conversely, a personal injury plaintiff was required to authorize the defendant to access private aspects of her Facebook and MySpace profiles because the court found she consented to have such information disclosed when she created these accounts, and the public aspects of her profiles revealed evidence that she was not injured and created a reasonable inference that her private pages contained similar evidence. *Romano v. Steelcase Inc.*, NY Slip Op. 20388, Case No. 2006-2233 (Sep. 21, 2010). In another example, the Justice Department secured a court order under the SCA allowing access to full Twitter streams of four individuals suspected to be involved with the WikiLeaks scandal. *In re Application of the United States*, No. 1:11-DM-00003, Dkt. No. 39 (March 11, 2011).

Summary of Statutes

This section summarizes provisions of some of the more relevant computer crime statutes: (1) the Electronic Communications Privacy Act (ECPA), (2) the Stored Communications Act (SCA), (3) the Computer Fraud and Abuse Act (CFAA), and (4) California's Comprehensive Data Access and Fraud Act, Penal Code Section 502 (Section 502). The section then describes data security and breach laws and lists some of the other laws relating to computer crimes. The following table illustrates the conduct prohibited by the four statutes addressed in more detail below, as well as the criminal and civil penalties available under such statutes.

Statute	Prohibited Conduct	Criminal Penalties	Civil Actions Allowed?	Damages	Attorneys' Fees	Punitive Damages
ECPA	Prohibits unlawful interception, use, and disclosure of communications in transit.	Fine and imprisonment	Yes	Actual damages and profits, or the greater of $100 per day for each violation or $10,000	Yes	Yes
SCA	Prohibits the unlawful disclosure of, and access to, communications in electronic storage.	Fine and imprisonment	Yes	Actual damages and profits, and at least a minimum of $1,000	Yes	Yes
CFAA	Prohibits hacking, unauthorized access, denial-of-service attacks, trafficking in passwords, and computer-based extortion, among other things.	Fine and imprisonment	Yes	Compensatory Damages	Not specified	Not specified
Section 502	Prohibits hacking, denial-of-service attacks, introducing malware, and email spoofing, among other things.	Fine and imprisonment	Yes	Compensatory Damages	Yes	Yes

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. §§ 2510-2522

The Electronic Communications Privacy Act (ECPA) provides specific protections for electronic communications. The ECPA is comprised of three titles. Title I, an amendment to The Wiretap Act, protects wire, oral, and electronic communications while in transit, and is addressed here. Title II, also known as the Stored Communications Act, protects communications held in electronic storage and is addressed in the next section. Title III prohibits the use of pen register and/or trap and trace devices to record certain information used in the process of transmitting wire or electronic communications without a court order. Title III is summarized in the last section below.

1. Prohibited Conduct

The Wiretap Act bars unauthorized individuals, and government agents acting without a warrant, from intentionally intercepting, using, or disclosing any wire and electronic communication while in transit, including telephone or cell phone conversations, pagers, voicemail, email and other computer transmissions. § 2511(1).

"Electronic communication" is defined (with some exclusions) as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." § 2510(12). Courts have held that "electronic communication" includes emails and other data such as drawings, pictures and sounds. "Wire communication" is defined to generally mean any aural (voice) transfer made through use of facilities for the transmission of communications by the aid of wire, cable or other like connection provided by a person engaged in providing such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce. § 2510(1) (s*ee United States v. Torres*, 751 F.2d 875, 886 (7th Cir. 1984) (silent television surveillance not interception of a wire communication because no human voice involved). Communications that do not affect interstate or foreign commerce are generally not implicated. §§ 2510(1),(12); *see United States v. Ropp*, 347 F. Supp. 2d 831, 835-38 (C.D. Cal. 2004) (transmissions of keystrokes from the computer to the central unit are not "electronic communications" because they "no more affected interstate commerce than a letter, placed in a stamped envelope, that has not yet been mailed;" computer is not a "system that affects interstate commerce or foreign commerce" simply because it is connected to an external network); *United States v. Scarfo*, 180 F. Supp. 2d 572, 582 (D. N.J. 2001); *but see Porter v. Havlieck*, No. 3:06-CV-211 2007 WL 539534 (S.D. Ohio Feb. 14, 2007) (finding that while keystrokes do not travel in interstate commerce, they do 'affect interstate commerce" and are therefore electronic communications); *Brahmana v. Lembo*, No. 09-C-00106, 2009 WL 1424438 (N.D. Cal. May 20, 2009) (denying as premature motion to dismiss finding that while complaint did not specify whether the particular means of monitoring might monitor keystrokes that actually affected interstate commerce, the issue of how any alleged monitoring took place and whether it allegedly affected interstate commerce is better resolved after discovery).

Intercept is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." § 2510(4). "[W]hen the contents of a wire communication are captured or redirected in any way, an interception occurs at the time." *United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992). An electronic communication must be in transmission to be "intercepted." *See Wesley College v. Pitts*, 974 F. Supp. 375, 385 (D. Del. 1997); *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 462 (5th Cir. 1994). Congress recently applied the transmission requirement to wire communications as well. *See* USA PATRIOT Act § 209, 115 Stat. at 283 (eliminating storage from the definition of "wire communication"); *see also Konop v. Hawaiian*

Airlines, Inc., 302 F.3d 868, 878 (2002) (Congress "approved the definition of 'intercept' as acquisition contemporaneous with transmission").

2. Exceptions

The prohibition against interception of wire and electronic communications has several exceptions, including for interception: (1) by providers protecting rights or property, (2) in the ordinary course of business, (3) where the parties to the communication consent, (4) of communications accessible to the public, and (5) by government authorities. These exceptions generally apply as follows.

a. Provider Exception

The Wiretap Act prohibits network service providers from intercepting or eavesdropping on a subscriber's email or other electronic or wire communication. However, it is not unlawful to intercept communications (1) while engaged in normal required job performance, and (2) for the protection of the rights or property of the provider of that service. § 2511(2)(a)(i); *see also United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir 1992) (provider exception allowed United Airlines to monitor online reservation system it provided to employees in an attempt to discover falsifications by a travel agent). This exception grants providers the right to conduct "reasonable" monitoring that balances the needs to protect their rights and property with the subscriber's or employee's right to privacy in their communications. *See United States v. Harvey*, 540 F. 2d 1345, 1351 (8th Cir. 1976); *United States v. Villanueva*, 32 F. Supp. 2d 635, 639 (S.D. N.Y. 1998) (providers have right to intercept and monitor communications placed over their facilities in order to combat fraud and theft of service); *United States v. Auler*, 539 F. 2d 642, 646 (7th Cir. 1976) (authority to monitor is not unlimited).

b. Business Use Exception

Private employers also enjoy an exception for use in the ordinary course of business. The Wiretap Act prohibits interception "through the use of any electronic, mechanical, or other device." § 2510(4). "[E]lectronic, mechanical, or other device" is defined, however, as a device or apparatus that can intercept communications *other than* "any telephone or telegraph instrument, equipment or facility" monitoring "in the ordinary course of its business." § 2510(5). A communication is therefore not intercepted if it is (1) accomplished through the use of a telephone or telegraph instrument, equipment, or facility, and (2) the monitoring was conducted in the ordinary course of its business. *See Deal v. Spears*, 980 F.2d 1153, 1157 (8th Cir. 1992); *Briggs v. American Air Filter Co.,* 630 F.2d 414, 420 (5th Cir. 1980) ("[W]hen an employee's supervisor has particular suspicions about confidential information being disclosed to a business competitor, has warned the employee not to disclose such information, has reason to believe that the employee is continuing to disclose the information, and knows that a particular phone call is with an agent to the competitor, it is within the ordinary course of business to listen in on an extension phone for at least so long as the call involves the type of information he fears is being disclosed."); *Williams v. Poulos*, 11 F.3d 271 (1st Cir. 1993) (no business use exception where employer used makeshift equipment to monitor calls, because such rigged devices are not considered ordinary business use).

c. Consent

The Wiretap Act provides that an interception is not unlawful ". . . where one of the parties to the communication has given prior consent to such interception . . . ." § 2511(2)(d); *In re Facebook Privacy Litig.*, No. 5:10-CV-02389 (N.D. Cal. May 12, 2011) (dismissing claim where Facebook users click on an advertisement is a communication to the intended recipient or with the lawful consent of, Facebook, and therefore not actionable). Consent can be express, or implied when the target knows or should have known

that their electronic communications would be intercepted. *Griggs-Ryan v. Smith*, 904 F.2d 112, 117-18 (1st Cir. 1990) (implied consent can occur where the surrounding circumstances show an acquiescence or knowledge of surveillance); *Griffin v. Milwaukee*, 74 F.3d 824, 827 (7th Cir. 1996) (holding that employee receiving emergency calls for police department had knowledge of possible interception of telephone calls and thus consented); *Deal v. Spears*, 980 F.2d 1153, 1151 (8th Cir. 1992) (knowledge of capability of monitoring can equal implied consent). The exception does not apply if the "communication is intercepted for the purpose of committing any criminal tortious act . . . ." § 2511(2)(d); *see also Caro v. Weintraub*, 2010 WL 3191353 *6 (2nd Cir. Aug. 13, 2010) (when one party to a conversation uses an iPhone to secretly record a conversation, it does not violate the WireTap Act, if the party at the time of the recording did not intend to commit a criminal or tortious act; "intent may not be inferred simply by demonstrating that the intentional act of recording itself constituted a tort"); *Sussman v. American Broadcasting Co.,* 186 F.3d 1200, 1201 (9th Cir. 1999) ("Where the taping is legal, but is done for the purpose of facilitating some further impropriety, such as blackmail, § 2511 applies. Where the purpose is not illegal or tortious, but the means are, the victims must seek redress elsewhere.")

d. Exception When Accessible to the Public

The Wiretap Act only protects electronic communications that are private, such as email and private electronic bulletin boards, as opposed to communications that are accessible to the public. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875 (9th Cir. 2002) (concluding, based on the ECPA's legislative history, that "Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards"); S. Rep. No. 99-541, at 36 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555-57 ("The bill does not for example hinder the development or use of 'electronic bulletin boards' or other similar services where the availability of information about the service, and the readily accessible nature of the service are widely known and the service does not require any special access code or warning to indicate that the information is private. To access a communication in such a public system is not a violation of the Act, since the general public has been 'authorized' to do so by the facility provider.").

e. Exception for Government Authorities

The Wiretap Act governs the circumstances under which law enforcement can intercept private communications. § 2518. In general, the government must obtain a special court order of limited duration (30 days), which may be granted if the judge finds that there is probable cause to believe the communications will yield evidence of a crime the target has committed or will commit. § 2518(3)(a).

3. Good Faith Defense

The Wiretap Act provides a complete defense to a civil or criminal action where there is a good faith reliance on: (1) a court warrant or order, a grand jury subpoena, or a legislative, or a statutory authorization; (2) a request of an investigative or law enforcement officer under section 2518(7) (procedure for interception of wire, oral, and electronic communications); or (3) a good faith determination that section 2511(3) or 2511(2)(i) permits the conduct complained of. § 2520(d).

4. Remedies

a. Civil

The Wiretap Act provides that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used" may bring a civil action to recover from the person or entity who engaged in

the violation. § 2520(a). For all actions except for private satellite video communication or certain radio communication, available relief includes equitable relief, damages, and reasonable attorneys' fees and costs. Damages are defined as either actual damages and profits, or whichever is greater between $100 per day for each violation or $10,000. § 2520(c). Punitive damages are also available. § 2520(b). The action must be brought within two years from the date of discovery of the violation or within two years from the time there was a reasonable opportunity to discover the violation. § 2520(e).

b. Criminal

Violations of the Wiretap Act are punishable by a fine and/or imprisonment of not more than 5 years. § 2511.

c. Exclusion of Evidence

The Wiretap Act also prohibits use of the contents of an unlawfully intercepted wire or oral communication, or any evidence derived there from, from being used as evidence in any trial or other court proceeding. § 2515. There is no similar exclusionary rule for electronic communications.

THE STORED COMMUNICATIONS ACT, 18 U.S.C. §§ 2701-2712.

The Stored Communications Act ("SCA") was passed as part of the ECPA and protects wire and electronic communications while in storage.

1. Prohibited Conduct

The SCA prohibits (1) unlawful access to certain stored communications, § 2701, and (2) unauthorized disclosure of stored communications by electronic communication services and remote computing services, § 2702. The SCA also limits the government's right to compel an electronic communications service or remote computing service to disclose information in their possession about their customers and subscribers. § 2703.

a. Unlawful Access to Stored Communications

With respect to access to stored communications, the SCA authorizes civil and criminal penalties against anyone who ". . . intentionally accesses without authorization a facility through which an electronic communication service is provided or . . . 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 . . . ." § 2701(a); *see Maremont v. SFDG*, 10-CV-07811 (E.D. Ill. Dec. 7, 2011) (denying summary judgment finding employer accessing personal Facebook and Twitter accounts, posting messages and accepting friend requests, raised a disputed issue as to whether exceeded authority). There are exceptions to this prohibition, including where the conduct is authorized by the provider of the electronic communications service or the user of the service with respect to a communication of, or intended for, that user. § 2701(c).

b. Unlawful Disclosure of Stored Communications

i. Prohibitions

With respect to disclosure of stored communications, the SCA prohibits providers of an "electronic communications service to the public" from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service." § 2702(a)(1). The SCA also prohibits providers of a "remote computing service to the public" from "knowingly divulg[ing] to any person or entity the contents of any communication which is carried or maintained on that service" "on behalf of and received by means of electronic transmission from . . . a subscriber or customer" where the communication is a customer communication received by means of electronic transmission and the provider is not authorized to access the contents. § 2702(a)(2). The SCA further prohibits a remote computing service or electronic communication service from knowingly divulging non-content information pertaining to a subscriber to any governmental entity. § 2702(a)(3).

ii. Limitations

This section expressly applies only to services provided "to the public." Services that are not provided to the public are not implicated by the statute. *See, e.g., Andersen Consulting LLP v. UOP,* 991 F. Supp. 1041, 1042 (N.D. Ill. 1998) (the SCA covers only entities that provide electronic communication services to the community at large).

Moreover, whether an entity is an "electronic communications service," a "remote computing service," or both, depends on the particular communication at issue. An electronic communications service is defined

as any service that offers to the public the ability to send or receive wire or electronic communications. § 2510(15). The definition also includes entities who provide electronic communications services even where they are ancillary to the company's main business or function. *See e.g., Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114-15 (3d Cir. 2004) (insurance company that provided email service to employees is an electronic communications service). However, businesses who use (as oppose to provide) an electronic communications service to sell traditional products or services online are generally not considered an electronic communications service. *See, e.g., In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 511, n. 20 (S.D. N.Y. 2001) (distinguishing Internet service providers that provide electronic communications service from websites that are users of electronic communications service).

Remote computing service, on the other hand, is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." § 2711(2). An electronic communications system is defined as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." § 2510(14); *see, e.g., Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256, 265 (S.D. N.Y. 2008) (YouTube is a remote computing service because it provides storage services for the user).

In some instances, one entity may be both an electronic communications service and a remote computing service, and the application of the SCA depends on the role that entity plays with respect to the particular communication at issue. *See, e.g., In re U.S.*, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009) ("Today, most ISPs provide both electronic communications services and remote computing services; thus, the distinction serves to define the service that is being provided at a particular time (or as to a particular piece of electronic communication at a particular time), rather than to define the service provider itself."); *United States v. Weaver*, 636 F.Supp.2d 769, 770 (C.D. Ill. 2009) (concluding that Microsoft, which provided email service through its Hotmail website, was both an electronic communications service and a remote computing service depending on whether emails were opened or unopened); *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010) (finding Facebook, MySpace, and Media Temple providers of electronic communications services with respect to un-opened private messages and providers of remote computing services with respect to opened and retained messages, wall postings, or comments); *but see In re Facebook Privacy Litig.*, No. 10-02389 (N.D. Cal. Nov. 22, 2011) (granting motion to dismiss finding "inconsistent" plaintiffs allegations that Facebook was an electronic communication service provider between users and advertisement and that Facebook was also a remote computing service, and that both theories fail).

The term "electronic storage" also has significance. Electronic storage is defined as "(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." § 2510(17). The first category of electronic storage applies when an electronic communications service temporarily stores a communication before delivering it. *Theofel v. Farey-Jones,* 359 F.3d 1066, 1075 (9th Cir. 2004). The second category, electronic communications stored for the "purposes of backup," is not defined in the statute and different cases have taken different approaches. *Cf. Theofel*, *supra,* 359 F.3d at 1075 (emails remaining on NetGate's server after delivery were for backup purposes should the user need to download them in the event emails were accidentally erased from the user's computer) *with Weaver, supra,* 636 F.Supp.2d 769, 772 (holding that once a user opens an email on Hotmail, a web-based email system, storing the opened message is not for backup purposes) and *Hilderman v. Enea TekSci, Inc.*, 551 F. Supp. 2d 1183, 1205 (S.D. Cal. 2008) (employee's storage of personal and private emails on hard drive of company laptop did not constitute "electronic storage" since emails

were not in temporary immediate storage and were not stored by electronic communications service for purpose of backup).

iii. Exceptions

There are exceptions to the prohibitions of the SCA. Electronic communications services can release private information to, or with the lawful consent of, "an addressee or intended recipient of such communication." §§ 2702(b)(1), (b)(3); *see In re Facebook Privacy Litig.*, No. 5:10-CV-02389 (N.D. Cal. May 12, 2011) (dismissing SCA claim where Facebook users click on an advertisement finding either Facebook is either the intended recipient and can consent, or the advertisers were the intended recipient and Facebook can divulge the communications to them); *Romano v. Steelcase Inc.*, NY Slip Op. 20388, Case No. 2006-2233 (Sep. 21, 2010) (by creating a Facebook and MySpace profile, plaintiff in personal injury action consented to the fact her personal information would be shared or become publicly available, notwithstanding privacy settings, and was ordered to deliver to the defendant authorization to access those records.) A remote computing service can release such information "with the lawful consent of . . . the subscriber." § 2702(b)(3). Both types of services can also disclose content information "to a person employed or authorized or whose facilities are used to forward such communication to its destination;" to law enforcement if the information was inadvertently discovered and pertains to the commission of a crime; when it is incidental to the rendition of services or to protect the rights and property of the provider; to a government entity upon a good faith belief of an emergency involving danger of death or serious bodily injury; or to the National Center for Missing and Exploited Children in connection with a submitted report. § 2702(b).

Electronic communication services and remote computing services are not prohibited under the SCA from disclosing non-content information without the consent of a customer to any other person or entity other than a governmental entity. § 2702(c)(6). Content "includes any information concerning the substance, purport, or meaning of that communication." § 2510(8). Non-content information includes a subscriber's name, address, billing records, sessions time and durations, length of service and types of services utilized, means and source of payment for the service, and "instrument number" which includes any temporarily assigned IP address and card or bank account number. § 2703(c)(1-2).

The SCA does not include an exception for disclosure pursuant to a civil discovery subpoena. *O'Grady v. Super. Ct.*, 44 Cal. Rptr. 3d 72 (2006) (court rejected Apple's attempt to obtain the email communications of an online journalist from a electronic service provider using a discovery subpoena); *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008) ("Applying the clear and unambiguous language of § 2702 to this case, AOL, a corporation that provides electronic communication services to the public, may not divulge the contents of the Rigsbys' electronic communications to State Farm because the statutory language of the [SCA] does not include an exception for the disclosure of electronic communications pursuant to civil discovery subpoenas."); *Bower v. Bower, et. al.*, 808 F. Supp. 2d 348 (D. Mass. 2011) (denying motion to compel Yahoo to comply with third-party document subpoenas because doing so would violate the SCA).

2. Good Faith Defense

The SCA provides a complete defense to a civil or criminal action where there is a good faith reliance on: (1) a court warrant or order, a grand jury subpoena, a legislative, or a statutory authorization; (2) a request of an investigative or law enforcement officer under section 2518(7) (procedure for interception of wire, oral and electronic communications); or (3) a good faith determination that section 2511(3) permits the conduct complained of. § 2707(e).

3. Remedies

a. Civil

Any "provider of an electronic communications service, subscriber, or other person aggrieved" may bring a civil action for violations of the SCA, and is entitled to seek preliminary and equitable or declaratory relief, damages, and reasonable attorney's fees and litigation costs. § 2707(a-b). Damages include "the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation." § 2707(c). Whether or not actual damages are shown, a person entitled to recover shall receive no less than the sum of $1,000. § 2707(c); *but see Van Alstyne v. Electronic Scriptorium, Ltd.,* 560 F.3d 199, 205 (4th Cir. 2009) (proof of "actual damages" is a prerequisite to recover statutory damages). One court has held that a damages award may be multiplied by the number of violations, but each violation does not necessarily warrant the separate statutory damage award. *See, e.g., In re Hawaiian Airlines, Inc.*, 355 B.R. 225, 232 (D. Hawaii 2006) (multiple visits to one website may functionally be a single visit, but violations separate in time that access different information would constitute separate violations entitled to separate damage awards). Punitive damages are available if the violation is willful or intentional. § 2707(c). The statute of limitations for a civil action is two years from the date of discovery or reasonable opportunity to discover. § 2707(f).

b. Criminal

The SCA provides for criminal penalties for unlawful access in violation of Section 2701. If the access is for "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," a first offender faces a fine and imprisonment of no more than 5 years, while a subsequent offender faces up to 10 years imprisonment. Access for all other purposes is punishable by a fine and up to 1 year imprisonment for first time offenders, and up to 5 years for recidivist offenders. § 2701(b).

4. Exclusive Remedy and Preemption

The SCA provides that "the remedies and sanctions described in this chapter are the only judicial remedies and sanctions for non-constitutional violations of this chapter." § 2708. "Only those remedies outlined in the SCA are the ones, save for constitutional violations [*e.g.*, fourth amendment], that a party may seek for conduct prohibited by the SCA. The SCA thus displaces state law claims for conduct that is touched upon by the statute, such as in divulging stored electronic communications to third parties." *Quon v. Arch Wireless Operating Co., Inc.,* 445 F. Supp. 2d 1116, 1137-38 (C.D. Ca. 2006) (affirmed in part, reversed in part on other grounds 529 F.3d 892, rehearing en banc denied 554 F.3d 769, certiorari granted 2009 WL 1146443, certiorari denied 2009 WL 1513112) (holding that the SCA completely preempts state law claims arising from conduct covered by the statute) (agreeing with *Muskovich v. Crowell*, 1995 WL 905403, at *1 (S.D. Iowa March 21, 2005) ("In section 2708, Congress unequivocally expressed an intent to 'occupy the field' and provide the exclusive remedies for conduct regulated by [SCA].")).

THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030

The Computer Fraud and Abuse Act (CFAA), enacted in 1984, was enhanced by several amendments including in 1996 through the National Information Infrastructure Protection Act, in 2001 through the USA PATRIOT Act, and in 2008 through the Identity Theft Enforcement and Restitution Act. The legislative history explains that the CFAA was enacted "to provide a clear statement of proscribed activity concerning computers to the law enforcement community, those who own and operate computers, and those tempted to commit crimes by unauthorized access to computers." S. Rep. No. 104-357 (1996); *see also e.g., P. Aerospace & Electronics, Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1194-95 (E.D. Wash. 2003) (describing the legislative history of the CFAA). CFAA claims are increasingly more common in the employment context, as are consumer class actions regarding collection and use of consumer information.

1. Prohibited Conduct

The CFAA prohibits unauthorized access to, damage to, or trafficking in passwords corresponding to federal government computers, financial institution computers, or computers used in interstate and foreign commerce. More specifically, the CFAA proscribes seven specific activities including : 1) obtaining national security information without authorization or in excess of authorized access from a computer; 2) obtaining information without authorization or in excess of authorized access from a financial institution computer, government computer, or protected computer; 3) intentionally accessing without authorization a government computer; 4) accessing a computer without authorization or in excess of authorized access with an intent to defraud and obtain value; 5) causing damage while either transmitting a program or intentionally accessing a protected computer; 6) trafficking in passwords with an intent to defraud; and 7) extortion involving threats to damage a protected computer. *See* 18 U.S.C. § 1030 (a)(1)-(7). In addition to prohibiting actual offenses, the CFAA also prohibits attempts to commit and conspiracy to commit offenses. *See* 18 U.S.C. § 1030 (b). The specific provisions of section 1030(a) are discussed in more detail as follows.

a. "Without Authorization" and "In Excess of Authorization"

Some of the prohibited conduct requires that the conduct be "without authorization" or "in excess of authorization." For example, Section 1030(a)(1) applies to both conduct performed "without authorization" or "exceeding authorized access," while Section 1030(a)(3) only applies to conduct "without authorization." The CFAA does not define the phrase "without authorization" but does define "exceeding authorized access" to mean "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." § 1030 (e)(6).

Recent developments under the CFAA involve the meaning and application of these terms in the employment context. While the phrase "without authorization" might appear to cover outside intruders and "exceeding authorized access" might appear to cover inside users, courts have differed in how strictly such distinctions are drawn. For example, some courts apply the phrase "without authorization" only to the activities of outside intruders who have not received permission to access a computer for any purpose. *See, e.g., LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1129 (9th Cir. 2009) (claim that an employee acted "without authorization" failed because employee had permission to access the company's computers). These courts reserve situations when an authorized individual, such as an employee, uses a computer for purposes beyond that which they are allowed to find they have "exceeded authorization." *See United States v. Nosal*, 642 F.3d 781, 785 (9th Cir. 2011) (holding that where an employee places limitations on an employee's use of the computer, use beyond that permission (i.e. into a restricted database) is with authorization but exceeds that authorization); *United States v. John*, 597 F.3d 263 (5th Cir. 2010) (holding an employee exceeded authorization when she accessed confidential customer information in violation of her

employer's computer use restrictions and used that information to commit fraud); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding an employee exceeded authorized access to obtain personal information for non-business reasons in violation of the company's policies); *EF Cultural Travel BV v. Explorica, Inc.,* 274 F.3d 577, 583-84 (1st Cir. 2011) (holding that an employee likely exceeded his authorized access when he used that access to disclose information in violation of a confidentiality agreement into which the employee voluntarily entered). Other courts, however, have held that an insider might in some instances act "without authorization" if they intend to act against the interests of the computer owner. *See, e.g.*, *Int'l Airport Center, LLC v. Citrin*, 440 F. 3d 418, 420-21 (7th Cir. 2006)(employee's breach of duty of loyalty to employer terminated employee's agency relationship with employee (and thus his authority to access) such that access was "without authorization"); *LKQ Corp. v. Thrasher*, 2011 WL 1984527, at *7 (N.D. Ill. May 23, 2011) (allegations of breach of employee duty of loyalty sufficient to allege accessed company computers without authorization); *Meridian Fin. Advisors Ltd. v. Pence*, 763 F. Supp. 2d 1046, 1062 (S.D. Ind. 2011) (allegations that employee deleted email in breach of duty of loyalty sufficient to allege without authorization). Further development in this area is likely to ensue, and Congress is currently considering an amendment that would clarify liability under the CFAA.

b. Obtaining National Security Information Without or in Excess of Authorized Access From a Computer. § 1030(a)(1)

Section 1030 (a)(1) of the CFAA prohibits (1) knowingly accessing a computer without authorization or in excess of authorized access, (2) and thereby obtaining information determined to require protection against unauthorized disclosure for reasons of national defense or foreign relations, (3) and delivering such information to anyone not entitled to receive it or willfully retaining the same with reason to believe that such information could be used to the injury of the United States or to the advantage of a foreign nation.

c. Obtaining Information Without or in Excess of Authorized Access From a Financial Institution Computer, Government Computer, or Protected Computer. § 1030(a)(2)

Section 1030 (a)(2) of the CFAA prohibits persons from "(1) intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and [(2)] thereby obtain[ing] (A) information contained in a financial record of a financial institution, or of a card issue . . . or contained in a file of a consumer reporting agency on a consumer . . . ; (B) information from any department or agency of the United States; or (C) information from any protected computer."

This section was originally enacted to protect individuals' computerized credit information at financial institutions, but was later expanded to protect information on government computers and protected computers. Section 1030 (e)(2) broadly defines the term "protected computer" as used in this provision and throughout the CFAA, as "a computer - exclusively for the use of a financial institution or the United States Government, or, . . .used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government;" or "*which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States*." (Emphasis added.)

The phrase "obtains information" has also been construed broadly to include the mere act of viewing information without copying or downloading such information. *AOL, Inc. v. National Health Care Discount, Inc.*, 121 F. Supp. 2d 1255, 1275-76 (N.D. Iowa 2000). Proof of violation of Section 1030 (a)(2) nevertheless requires a showing that the person charged actually "accessed" a computer in addition to the other proscribed activity. *See Role Models America Inc. v. Jones*, 305 F. Supp. 2d 564, 567-68 (D. Md. 2004).

d. Intentionally Accessing Without Authorization a Government Computer § 1030(a)(3)

Section 1030 (a)(3) of the CFAA prohibits accessing, without authorization, a nonpublic computer of a department or agency of the United States where the computer is exclusively for use of the government, or is used by the government and such conduct affects that use by or for the government. In essence, this section criminalizes trespass to non-public government computers. The modifying phrase "non-public" was added by amendment to narrow the scope of this section to avoid prosecution for access to government computers available to the public, such as web servers. Similarly, omission of the phrase "exceeding authorized access" appears to be a purposeful attempt to limit the scope to intruding outsiders and not to unwittingly ensnare insider federal employees in federal prosecution.

e. Accessing a Computer Without or In Excess of Authorized Access With an Intent To Defraud and Obtain Value. § 1030(a)(4)

Section 1030 (a)(4) prohibits "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period."

This section requires proof of "intent to defraud," which is not defined by the CFAA, but courts have interpreted this phrase to mean proof of "wrongdoing," rather than to require proof of each of the elements of common law fraud. *See eBay Inc. v. Digital Point Solutions*, *Inc.*, 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009); *Shurgard Storage Centers, Inc., v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1124-26 (W.D. Wash. 2000). This section additionally requires proof that the unauthorized access "furthers the intended fraud," and such proof can be satisfied in a number of ways. *See, e.g., United States v. Butler*, 16 Fed. Appx. 99 (4th Cir. 2001) (altering credit rating to receive something of value based on the modified records); *United States v. Lindsley*, 254 F.3d 71 (5th Cir. 2001) (obtaining and using calling card numbers that are used to commit fraud); *United States v. Bae*, 250 F.3d 774, 775 (D.C. Cir. 2001) (using a lottery terminal to back-date winning lottery tickets that are used to commit fraud).

Section 1030(a)(4) also requires proof that the accused obtained something of value or, if the object of the fraud and the thing obtained is computer use, the value of the computer use meets or exceeds $5,000 in a one-year period. For example, the court in *United States v. Czubinski*, held that an IRS employee who merely exceeded his authorized access to review taxpayer files in order to satisfy his curiosity, without using this information to further an intended fraudulent scheme, did not satisfy the elements of this provision since the value of such use did not exceed $5,000 in a one-year period. *See* 106 F3d 1069, 1078-79 (1st Cir. 1997). In contrast, the court in *NCMIC Finance Corp. v. Artino* held that when an employee emailed himself the company's customer list for personal gain in conflict with the company's interest, the customer list was "something of value" that could exceed $5,000 in a one-year period. *See* 638 F. Supp. 2d 1042, 1062-63 (S.D. Iowa 2009). Similarly, the court in *In re America Online, Inc.* held that AOL's provision of software, which blocked competitor's software in an alleged furtherance of securing AOL's stronghold as an Internet service provider resulted in AOL obtaining something of value under Section 1030 (a)(4) because "AOL's actions have interfered with [the plaintiff's] relationships with its existing customers and potential subscribers." *See* 168 F. Supp. 2d 1359, 1380 (S.D. Fla. 2001).

f. Causing Damage While Transmitting a Program or Intentionally Accessing a Protected Computer. § 1030(a)(5)

Section 1030 (a)(5) prohibits "(A) knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer; (B) intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage; or (C) intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss." Section 1030(a)(5) addresses computer crash attacks, denial-of-service attacks, and installation of malware such as computer viruses or worms.

The "transmission" element of Section 1030 (a)(5)(A) has been construed to include both direct and indirect sending of a program through the Internet to a computer network and copying a program from one computer to another via a disk drive. *See, e.g., United States v. Sullivan*, 40 Fed. Appx. 740, 741 (4th Cir. 2002) (act of inserting malicious code into a computer network, even if it lays dormant for several months, violates Section 1030 (a)(5)*; see also Int'l Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 419-20 (7th Cir. 2006) ("knowingly causes the transmission" element satisfied even if the copying is accomplished only through a disk drive). Additionally, courts have construed the "intentionally accesses" phrase to include not only circumstances where the accused accesses protected computers using passwords, but also those acts where the accused uses automated programs to thwart computer security in order to gain access. *See United States v. Morris*, 928 F.2d 504, 509-10 (2d Cir. 1991); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 249, 251 (S.D.N.Y. 2000). Moreover, because both Sections 1030 (a)(5)(B) and (C) require proof of intentional access of a protected computer "without authorization," these two sub-sections are seemingly directed to outside intruders rather than authorized users exceeding their authorization.

The proof of injury is slightly different in each of the sub-sections of Section 1030 (a)(5). While Sections 1030 (a)(5)(A) and (a)(5)(B) require only proof of "damage," Section 1030 (a)(5)(C) requires proof of "loss" in addition to "damage." Notably, however, Section 1030 (a)(5)(B) and (C) do not require that the "damage" be caused to the same protected computer that was intentionally accessed without authorization.

g. Trafficking In Passwords With Intent to Defraud. § 1030(a)(6)

Section 1030 (a)(6) prohibits: "knowingly and with intent to defraud traffic[king] (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—(A) such trafficking affects interstate or foreign commerce; or (B) such computer is used by or for the Government of the United States; . . ."

While the term "password" may ordinarily be considered to consist merely of a text-string that a user enters to log in to a computer or use to access a bank account, the term is broader under Section 1030(a)(6) and includes more complex instructions such as a set of access commands. Also, while proof of actual trafficking in a password - as opposed to mere possession - is required for a violation to be found, proof of a profit motive is not. Moreover, the term "traffic," as defined in 18 U.S.C. § 1029 (e)(5) "means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of." Thus a violation may be shown even where the password has not been transferred or disposed of so long as the intent to transfer or dispose of the password can be shown.

The phrase "affects interstate or foreign commerce" is not statutorily defined, but courts have held that the phrase includes conduct involving a computer "'providing a web-based' application accessible through the Internet." *United States v. Drew,* 259 F.R.D. 449, 457-58 (N.D. Cal. 2009) (citations omitted).

h. Extortion Involving Threats to Damage a Protected Computer. § 1030(a)(7)

Section 1030 (a)(7) prohibits: "with intent to extort from any person any money or other thing of value, transmit[ting] in interstate or foreign commerce any communication containing any— (A) threat to cause damage to a protected computer; (B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or (C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion."

Section 1030(a)(7), added by amendment in 1996, protects against computer-based extortion and follows the same general guidelines provided in prior federal extortion statutes. *See United States v. Ivanov*, 175 F. Supp. 2d 367, 372 (D. Conn. 2001) (comparing Section 1030 (a)(7) with the Hobbs Act, 18 U.S.C. § 1951). While the threat of extortion must be transmitted in interstate or foreign commerce under Section 1030 (a)(7), the threat does not have to be communicated via computer.

2. Exceptions

The CFAA provides statutory exceptions for "lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States." *See* § 1030 (f).

Additionally, the CFAA "creates only a limited private right of action 'against the violator,' that is, against a person who violates the statute with the requisite criminal intent." *Doe v. Dartmouth-Hitchcock Med. Ctr.,* 2001 WL 873063 (D.N.H. July 19, 2001) (declining to expand the cause of action "to include one for vicarious liability against persons who did not act with criminal intent"); *but see Charles Schwab & Co.. v. Carter*, 2005 W.L. 2369815 at *5 (N.D. Ill. Sept. 27, 2005) (holding that vicarious liability may exists against competitors who affirmatively encourage an employee to access their former employer's computer system without authorization).

3. Penalties

a. Civil

The CFAA permits civil claims in some instances by persons who suffer "damage or loss by reason of a violation of the CFAA." Recovery under such claims includes compensatory damages, and injunctive or other equitable relief. The challenged conduct must cause either (i) a loss of at least $5,000 during a one-year period, (ii) physical injury, (iii) a threat to public safety, (iv) damage to a national security computer, (v) or damage to at least ten protected computers during a one-year period. For actions under the first prong, damages are limited to economic damages - which the CFAA does not define but which generally refer to non-speculative monetary loss, cost to repair, or loss of property. Generally 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. *See* § 1030 (g).

The past few years has seen continued development of the meaning of "damage" and "loss" under the statute. Section 1030 (e)(8) defines "damage" to mean "any impairment to the integrity or availability of data, a program, a system, or information." Damage may therefore be shown in the circumstance where an unauthorized user changes the way a computer operates, deactivates security software, or makes a computer seem unusable or unavailable. *See, e.g., United States v. Middleton*, 231 F.3d 1207, 1213-14 (9th Cir. 2000) (deactivation of computer security). Damage can also be proven by showing that data was

accessed or copied, even without altering or deleting any data on a computer or system. *See, e.g., Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.,* 199 F. Supp. 2d 1121, 1126-27 (W.D. Wash. 2000). There is a limit, however, as to what will constitute as damage. For example, one court found that temporary loss of cell phone service does not constitute damage. *See In re Apple & ATTM Antitrust Litigation,* No. 07-05152, p. 10-11 (N.D. Cal. July 8, 2010). Moreover, while there is no express proximate causation requirement, at least one court has held that the injury need be "a natural and foreseeable result of any damage." *United States v. Middleton*, 231 F.3d 1207, 1213 (9th Cir. 2000).

As distinct from "damage," Section 1030 (e)(11) defines "loss" to mean "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." Proof of loss may be shown by the wages paid to computer programmers and system administrators to restore the information or computer system to its original condition, and also includes the wages due to installing further computer security measures. *See e.g., EF Cultural Travel v. Explorica, Inc.*, 247 F.3d 577, 584 at n.17 (1st Cir. 2001). Loss can also be the cost of monitoring records and of audits conducted as part of the damage assessment. *See, e.g., United States v. Janosko*, 642 F.3d 40, 42 (1st Cir. 2011) (monitoring credit records due to accessed information was a "cost of responding to an offense" and therefore compensable); *Univ. Sports Publ'ns Co. v. Playmakers Media Co.*, 725 F. Supp. 3d 378, 388 (S.D. N.Y. 2010) (cost of audit to investigate a loss). However, "the CFAA does not recognize lost revenue damages as 'loss' unless it was 'incurred because of interruption of service." *See, Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 642, 653 (E.D. Va. 2010) (citations omitted); *CoStar Realty Info., Inc. v. Field*, 737 F. Supp. 2d 496, 509 (D. Md. 2011) (loss based solely on lost revenue unrelated to interruption of service "is insufficient to qualify as a loss");*see also SKF USA, Inc. v. Bjerkness*, 636 F. Supp. 2d 696, 721 (N.D. Ill. 2009) ("Costs not related to computer impairment or computer damages are not compensable under the CFAA."); *Lee v. PSMI*, No. 8:10-CV-2904 (M.D. Fla. May 6, 2011) (loss of employee productivity because employee was checking Facebook at work was not loss); *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935-36 (9th Cir. 2004) (loss of business and loss of goodwill are economic damages under the CFAA); *Register.com v. Verio, Inc.* 126 F. Supp. 2d 238, 252 n. 12 (S.D.N.Y. 2000), *aff'd* 356 F.3d 393 (2d Cir. 2004) (loss of advertising revenue or lost sales).

b. Criminal

Criminal penalties under the CFAA range from modest fines and jail time to large fines and imprisonment for 20 years to life. *See* § 1030 (c). On the lower end of the spectrum, the CFAA generally specifies criminal penalties of a fine or imprisonment of not more than one year for first offenses and low value or low damage crimes. The CFAA, however, permits harsher sentences for some first offenses, for example, for violations of Sections 1030 (a)(1), (a)(4), (a)(5)(A), and (a)(7). On the higher end of the spectrum, the CFAA specifies much higher penalties for recidivist conduct or attempts to cause bodily injury.

Moreover, some sections of the CFAA have been enhanced by the passage of other laws. For example, section 1030(a)(1) is also listed as a Federal Crime of Terrorism in the USA PATRIOT Act, which extends the statute of limitations to eight years and allows prosecution under the RICO Statute.

CALIFORNIA'S COMPREHENSIVE DATA ACCESS AND FRAUD ACT (CAL. PENAL CODE SECTION 502)

California's Comprehensive Data Access and Fraud Act, Penal Code Section 502 (Section 502) is designed to expand the degree of protection afforded to individuals, business, and governmental agencies from tampering, interference, damages, and unauthorized access to lawfully created computer data and computer systems. *See* Section 502(a).

1. Prohibited Conduct

Section 502 prohibits computer crimes involving computer hacking, email spoofing, denial-of-service attacks, and introduction of malware and other computer viruses into a computer or computer system.

Specifically, Section 502(c) prohibits:

- Knowingly access[ing] and without permission alter[ing], damag[ing], delet[ing], destroy[ing], or otherwise us[ing] any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data. Section 502 (c)(1).
- Knowingly access[ing] and without permission tak[ing], cop[ying], or mak[ing] use of any data from a computer, computer system, or computer network, or tak[ing] or cop[ying] any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network. Section 502 (c)(2).
- Knowingly and without permission us[ing] or caus[ing] to be used computer services. Section 502 (c)(3).
- Knowingly access[ing] and without permission add[ing], alter[ing], damag[ing], delet[ing], or destroy[ing] any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network. Section 502 (c)(4).
- Knowingly and without permission disrupt[ing] or caus[ing] the disruption of computer services or den[ying] or caus[ing] the denial of computer services to an authorized user of a computer, computer system, or computer network. Section 502 (c)(5).
- Knowingly and without permission provid[ing] or assist[ing] in providing a means of accessing a computer, computer system, or computer network in violation of this section. Section 502 (c)(6).
- Knowingly and without permission access[ing] or caus[ing] to be accessed any computer, computer system, or computer network. Section 502 (c)(7).
- Knowingly introduc[ing] any computer contaminant into any computer, computer system, or computer network. Section 502 (c)(8).
- Knowingly and without permission us[ing] the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damag[ing] or caus[ing] damage to a computer, computer system, or computer network. Section 502 (c)(9).

The prohibited acts under Section 502 generally track the prohibited acts under the CFAA.

Sections 502 (c)(1), (c)(2), and (c)(4) all require proof that accused "access" data from a computer, computer system, or computer network. The term "access" is defined to mean "to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network." Courts have held that the provisions of Section 502 (c) that require proof that a person knowingly access and without permission alter, delete, or use data do not apply to those who have merely exceeded their authority to access such data. *See, e.g.*, *Chrisman v. City of Los Angeles*, 155 Cal. App. 4th 29, 37 (2007); *Mahru v. Superior Court*, 191 Cal. App. 3d 545, 448-49 (1987) (declining to apply Section 502 (c)(4) to a data processing employee who had access, but purportedly exceeded such access).

All of the prohibited acts listed in Section 502 (c) require the conduct be committed "knowingly," and courts have held that this requires that every action described in the statute be undertaken with intent. In other words, "knowingly" modifies the entire prohibition under each provision listed in Section 502 (c), not just the act of accessing. *See People v. Hawkins*, 98 Cal. App. 4th 1428, 1438-39 (2002) (inclusion of "knowingly" in statute requires *mens rea* and does not create a strict liability offense).

It should also be noted that some of the prohibitions under Section 502 appear particularly broad. For example, Section 502 (c)(7) prohibits any unauthorized person from "knowingly and without permission accessing or causing to be accessed any computer, computer system, or computer network." There is no requirement that any data be taken or altered. Instead, proof of unauthorized access is all that need be shown.

Two recent *Facebook* cases came to opposite conclusions in addressing whether violating a website terms of service is sufficient to meet the "without permission" requirement of Section 502. *See, e.g. Facebook, Inc. v. ConnectU LLC*, 489 F. Supp. 2d 1087, 1090-91 (N.D. Cal. 2007) (holding that competitor violated Section 502 when it accessed Facebook in violation of the terms of use); *Facebook, Inc. v. Power Ventures, LLC*, 2010 WL 3291750, *7-9, 12 (N.D. Cal. July 20, 2010) (applying the logic followed in California cases concerning the CFAA and finding competitor's actions in violation of terms of use, which did not overcome technical or code-based barriers, did not meet the "without permission" requirement). However, court have found that when a "party accesses the network in a manner that circumvents technical or code-based barriers in place to restrict or bar a user's access," then that access is "without permission." *See Facebook, Inc. v. Power Ventures, LLC*, Dkt. 275 (N.D. Cal. Feb. 16, 2012) (Facebook secured summary judgment for violations of the CFAA and Section 502, finding the access was without authorization because code designed to circumvent barriers); *Facebook Privacy Litigation*, No. 5:10-CV-02389 (N.D. Cal. May 12, 2011) (granting motion to dismiss section 502 action where there was "clearly no technical barriers blocking [Facebook] from accessing its own website").

2. Exceptions

Section 502 (h)(1) recites an exception to liability for persons performing reasonably necessary acts within the scope of his or her lawful employment. Moreover, Section 502 (h)(2) provides that a person will not violate the expansive scope of Section 502 (c)(3) if the person is "acting outside of his or her lawful employment, provided that the employee's activities do not cause an injury . . . to the employer or another . . . ." or provided that the value of supplies or computer services at issue does not exceed $250. *Chrisman v. City of Los Angeles*, 155 Cal. App. 4th 29, 37 (2007) (subdivision 502(h)(2) renders police officer's conduct noncriminal because he did not damage employer's computer).

3. Penalties

a. Civil

Section 502(e) provides for private plaintiffs to bring civil actions for commission of acts prohibited by Section 502 (c). Plaintiffs filing such actions may seek and receive injunctive relief as well as compensatory damages. Moreover, such relief is not exclusive of other civil remedies available. Damages also include "any expenditure reasonably and necessarily incurred . . . to verify that a computer system . . . was or was not altered, damaged, or deleted by the access." *See* §502(e)(1). "Section 502 sets no threshold level of damage or loss that must be reached to impart standing to bring suit." *Facebook, Inc. v. Power Ventures, LLC*, 2010 WL 3291750, *4 (N.D. Cal. July 20, 2010) ("any amount of damage or loss may be sufficient"). Notably, where the conduct is committed by an unemancipated minor, liability shall be imputed to the parent or legal guardian. See § 502 (e)(1), (2).

The court may also award punitive or exemplary damages for willful violations (*i.e.*, crime including guilt of oppression, fraud, or malice proved by clear and convincing evidence). *See* §502 (f)(4). Reasonable attorney's fees are also recoverable. *See* §502 (e)(2).

b. Criminal

Section 502(d) imposes criminal penalties ranging from fines not exceeding $1,000 and no prison term to fines of $10,000 and 2-3 years in state prison depending on the applicable provision, the severity of the injury caused, and whether the violation was the first or a subsequent violation. Also, according to Section 502(g), any computer or computer system owned by the defendant that is used during commission of any offense described in Section 502 (c) is subject to forfeiture.

LAWS REQUIRING DATA SECURITY AND BREACH NOTIFICATION

A question that often arises in instances of a computer crime is notification of those affected by such a crime. A majority of states have enacted security breach notification laws, and some states have supplemented those laws with laws requiring consumer information to be maintained in a secure fashion. There is no Federal security breach notification statute, though the FTC has enforced claims for security breaches based on breaches of privacy policies and unfair competition.

California was the first state to enact a security breach notification law. California Code of Civil Procedure section 1798.82(a) requires that "[a]ny person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." The statute requires specific types of notice, among others things. The laws of other states are generally similar to the California statute, but have different requirements that need to be reviewed in connection with breaches and breach notification.

California Code of Civil Procedure section 1798.81.5(b) requires that "[a] business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." The statute also requires such companies to require similar protections in contracts with those with whom they do business, among other things. Other states have passed similar laws, with Massachusetts' Data Security Regulations being one of the most comprehensive. The FTC has also imposed a Red Flags Rule, which requires certain companies to identify data breach risks and have a plan to address such risks.

OTHER COMPUTER CRIME RELATED LAWS

1. Federal Statutes

a. The Economic Espionage Act, 18 U.S.C. § 1831-39

Addresses trade secret misappropriation generally and makes it a crime to knowingly commit an offense that benefits a foreign government or a foreign agent. Punishment for a violation is a fine of up to $250,000 and imprisonment of up to 10 years, or both.

b. Fraud in Connection with Access Device, 18 U.S.C. § 1029

Criminalizes fraud and related activity performed to obtain a thing of value and in connection with access devices. Punishment includes fines and jail time ranging in amount and severity based on conduct.

c. Fraudulent Online Identity Sanctions Act, 15 U.S.C. §1051

Increase criminal penalties for those who submit false contact information when registering a domain name that is subsequently used to commit a crime or engage in copyright or trademark infringement.

d. Identity Theft and Assumption Deterrence Act, 18 U.S.C. § 1028(a)(7)

Criminalizes eight types of conduct involving fraudulent identification documents or the fraudulent use of identification information. While the CFAA covers aspects of identity theft as well, the ITADA addresses restitution and relief for victims. Punishable by a fine or imprisonment of up to 15 years, or both.

e. Mail and Wire Fraud, 18 U.S.C. § 1341, 1343

Prohibits schemes to defraud or obtain money or other property, including trade secrets and other confidential and proprietary information, using the United States Postal Service or wire, radio, television communications. Punishable by a fine of up to $250,000 and imprisonment of up to 5 years, or both.

f. National Stolen Property Act, 18 U.S.C. §§ 2311-33

Prohibits the receipt, sale, or transportation of stolen goods, wares, merchandise, security, or money. The stolen goods must have a value of $5,000 or more. Punishment for a violation is a fine of up to $250,000 and imprisonment of up to 10 years, or both.

g. Pen Register/Trap & Trace Statute, 18 U.S.C. §§ 3121-3127

This statute is Title III of the ECPA, and prohibits a third party, including the government, from using tracking devices to intercept wire or electronic communications, without first obtaining a court order. 18 U.S.C. § 3121(a). The statute expressly prohibits tracking devices from collecting communications content. § 3127(3) ("shall not include the contents of a communication"); *see also People v. Bialostok*, 610 N.E. 2d 374, 378 (N.Y. Ct. App. 1993) (devices that can acquire communications contents cannot be authorized under Pen/Trap statute). A court order can allow surveillance of non-content information, including when and with whom a person communicates using email, instant messaging, text messaging, telephone, and the IP addresses of the websites an individual visits. § 3121(a).

h. Digital Millennium Copyright Act, 17 U.S.C. §§ 1201-1205

Prohibits, among other things, circumventing a technological measure (such as copy protection on CDs, product code, etc.) designed to protect a copyright and prohibits the manufacture or sale of devices or programs whose primary purpose is to circumvent access control technology. The DMCA also prohibits the removal or alteration of information identifying the author, copyright holder, performer, or director of a work, and terms and conditions for use of a work for the purpose of facilitating copyright infringement. The act provides for civil and criminal penalties.

2. Selected State Statutes

a. Uniform Trade Secrets Act (UTSA)

The UTSA is a model law adopted in almost all states, and prohibits misappropriation of a trade secret. The UTSA generally allows a private cause of action for the victim, who is entitled to injunctive relief, damages, including "exemplary" damages, and reasonable attorneys' fees if the misappropriation was in bad faith or willful or malicious.

b. California Wiretap Act, Cal. Penal Code §§ 630-38

Criminalizes interception of or eavesdropping upon any confidential communication without the consent of all parties. *See Kearney v. Smith Barney, Inc.*, 39 Cal. App. 4th 95 (one party consenting is not enough). It is also a crime to disclose information obtained from eavesdropping. A first offense of eavesdropping is punishable by a fine of up to $2,500 and imprisonment for no more than one year, and subsequent offenses carry a maximum fine of $10,000 and jail sentence of up to one year. Intercepting, recording and disclosing information each may involve a separate penalty. Anyone injured by a violation can recover civil damages of $5,000 or three times actual damages, whichever is greater, and seek injunctive relief.

c. Massachusetts Computer Crime Legislation, Mass. Gen. Laws. ch. 266, §§ 30, 33(A), 60(A), 160 (1995)

Provides criminal penalties for theft of an electronically stored trade secret, obtaining computer services by fraud or misrepresentation, buying or selling trade secrets, and unauthorized access to a computer system, directly or by network or telephone. The law also defines electronically stored or processed data as "property" under the criminal vandalism statute.

d. New York Penal Code, N.Y. Penal Law § 156

Criminalizes offenses involving computers, including unauthorized use, trespass, tampering, unlawful duplication of computer related material, and criminal possession of computer related materials.

e. Texas Computer Crimes and Telecommunications Crimes, Texas Penal Code § 33(A)

Prohibits the unauthorized use of protected computer systems or data files on computers, and intentional harmful use of such computers or data files. The statute prohibits similar conduct with respect to telecommunications systems.

f. Virginia Computer Crimes Act, Va. Code §§ 18.2-152.1

Provides for civil penalties for computer fraud, computer trespass, computer invasion of privacy, theft of computer services and computer forgery.

g. Washington, Was. Rev. Code §§ 926A.110, 9A.48, 9A.52, 9A.56

Criminalizes fraud in obtaining telecommunications service, computer trespass, theft of telecommunication services, and unlawful manufacture/sale of a telecommunication device, among others.

Author Contacts

James G. Snell
Partner
Bingham McCutchen LLP
1900 University Avenue
East Palo Alto, CA 94303
james.snell@bingham.com

Jim Snell is co-chair of Bingham's Privacy and Security Group and former co-chair of the firm's Intellectual Property Group. Jim represents clients in a broad range of complex commercial matters, including patent litigation, Internet and privacy issues, trade secret matters, matters involving unfair competition claims under California Business and Professions Code section 17200, false advertising, and class actions. He has particular experience in privacy, Internet and marketing issues, including junk email laws, spyware issues, matters involving the Telephone Consumer Protection Act, and data security issues. He defended the first lawsuit filed under the CAN-SPAM Act as well as the first lawsuit filed under Michigan's Child Protection Registry. Jim has also handled cases involving novel issues of Internet law relating to the Communications Decency Act.

Heather Shook
Associate
Bingham McCutchen LLP
1900 University Avenue
East Palo Alto, CA 94303
heather.shook@bingham.com

Heather Shook advises clients on general litigation matters, including matters involving computer crimes. Prior to joining the firm, she worked for a defense team at the International Criminal Tribunal for the Former Yugoslavia in the Hague, Netherlands. Heather also served as a extern for the Hon. John Noonan at the United States Court of Appeals, Ninth Circuit.

Peter R. Vogel
(Former Associate)

Peter Vogel is Senior IP Counsel at Alcatel-Lucent.