WHERE HAS ALL OUR PRIVACY GONE?

Carol M. Bast[*]
Cynthia A. Brown[**]

> If you want to know the law and nothing else, you must look at it as a bad man, who cares only for the material consequences which such knowledge enables him to predict, not as a good one, who finds his reasons for conduct, whether inside the law or outside of it, in the vaguer sanctions of conscience.[1]

I. INTRODUCTION

Privacy is much like a mirage on the horizon, an illusion that seems real at a distance but that becomes fainter as we examine it more closely. At some point in the twentieth century we thought that we had privacy in what we said, did, and where we went; although this belief may not have been totally grounded in reality.[2] The reality is that technology existed during this last century that could be used by one, like Oliver Wendell Holmes' bad man,[3] who wished to ferret out what we thought we could keep safe from prying eyes and ears.

With changes in society and advances in technology, it appears what little privacy we could claim in reality in the twentieth century is a vanishing commodity. Our telephone conversations and digital communication may be monitored; our actions may be recorded by cameras on the streets; and our travels may be monitored by the global positioning system (GPS). Our communication privacy is constantly under assault by technology and may be captured by competitors,[4] thieves,[5] or the

[*] Associate Professor, Department of Legal Studies, University of Central Florida, Orlando, Florida 32816; 407 823-5364; email: carol.bast@ucf.edu.
[**] Assistant Professor, Department of Legal Studies, University of Central Florida, Orlando, Florida 32816; 407-823-1670.
[1] O. W. Holmes, *The Path of the Law*, 10 HARV. L. REV. 457, 459 (1897). *See infra* notes 137-38, 140-43, 161-63 and accompanying text.
[2] Westin's seminal work, ALAN F. WESTIN, PRIVACY AND FREEDOM (1967), was published forty-five years ago. Although perhaps not of common knowledge, technology had made significant inroads on privacy. For Westin, some "new tools" for penetrating one's privacy included a miniature radio-signal transmitter that could pinpoint the target's location, a miniature hidden camera, a directional or spike microphone able to hear conversations in a closed room by measuring vibrations transmitted through walls or structures providing utilities, and the induction coil used to wiretap without penetrating telephone wires. *Id.* at 69-78.
[3] *See* Holmes, *supra* note 1 and accompanying text and *infra* notes 137-38, 140-43, 161-63 and accompanying text.
[4] "Because the United States is a leader in the development of new technologies and a central player in global financial and trade networks, foreign attempts to collect US technological and economic information will continue at a high level and will represent a growing and persistent threat to US economic security." OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, FOREIGN SPIES STEALING US ECONOMIC INTERESTS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 2009 – 2011 i (2011), *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf. This October 2011 report emphasizes that technology facilitates this ever-growing threat. "The nature of the cyber threat will evolve with continuing technological advances in the global information environment." *Id.*

curious, all without our consent or knowledge.[6] Given the technology-equipped workplace, employers gather much of our personal information, perhaps with our grudging consent.[7]

By overt acts, we willingly turn over much of our valuable information to third parties, such as telecommunications companies and banks; this contrasts with information gathered surreptitiously by third parties without our consent or knowledge. As we make more extensive use of communication technology, the possibility of surreptitious third-party surveillance increases, with surveillance technology almost keeping pace with advances in communication technology.[8] Communication privacy is constantly under attack from technological advances and the general effect of pervasive communication interception is to chill free speech. The special effect of the interference is to play havoc with the individual's personal life.

Examples of the manner in which our privacy is being eroded include cell phones being used as microphones,[9] software capturing key strokes,[10] and sniffer software intercepting Wi-Fi data.[11] We are almost at a tipping point, in that technology has become all-pervasive without our conscious recognition. Technology is suspended from one end of the balance beam arm and our privacy is suspended from the other end of the arm. At the present, the arm is out of equilibrium, with technology more weighty than our privacy. When greater emphasis is placed on privacy, the arm will move into a horizontal position to a tipping point, where, with a little more weight on the privacy side of the arm, the

---

[5] Businesses with sensitive data may be especially vulnerable. An October 2011 report outlines an alarming danger for the economic wellbeing of United States businesses. "Foreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security." *Id.* Technology facilitates this danger. "Cyberspace—where most business activity and development of new ideas now takes place—amplifies these threats by making it possible for malicious actors, whether they are corrupted insiders or foreign intelligence services (FIS), to quickly steal and transfer massive quantities of data while remaining anonymous and hard to detect." *Id.*

[6] Movie stars discover that their conversations have been intercepted when an article appears in the press or someone is indicted. John F. Burns, *Phone Hacking Charges Seen as Chill on British Journalism*, N.Y. TIMES, July 24, 2012, *available at* http://www.nytimes.com/2012/07/25/world/europe/two-ex-editors-for-murdoch-to-be-charged-for-phone-hacking.html?pagewanted=all. Recently, a Florida man pleaded guilty to illegally accessing the email accounts of over fifty entertainment personalities using information publicly available on the internet. *Hacktastic*, NAT'L L.J., Apr. 2, 2012, at 2.

[7] *See, e.g. City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010). For a discussion of *Quon*, *see infra* notes 151-55. For example, employers and potential employers may search social media sites to investigate employee and potential employee activities. Some of the employee information at the sites is freely available, and the employer may demand login information as a condition precedent to considering the person's employment application or as a condition of continued employment. A further discussion of employee loss of privacy through access to social media site information is beyond the scope of this article.

[8] *See infra* notes 17-34 and accompanying text.

[9] *See infra* notes 17-21 and accompanying text.

[10] *See infra* notes 22-27 and accompanying text.

[11] *See infra* notes 28-34 and accompanying text.

individual will regain privacy. The tipping point will come when there is a business or consumer movement to restore the status quo of having the communicator in control of the communication. Perhaps this will lead to legislation or the widespread use of defensive technology.

This evaporation of communication privacy is exacerbated by the fact that much communication interception goes undetected and statutes that we may assume protect our privacy are woefully out of date.[12] At the same time, courts have been reluctant to protect privacy in the face of technological advances.[13] Federal and state statutes may very likely be found by courts not to apply to many types of advances in technology, leaving the individual with an increasingly shrinking realm of privacy. We have allowed privacy to slip away. Now is the time to be active in defending our communication privacy. If we are not willing to accept this erosion in privacy as the new social norm, we must be proactive in combating this threat. The solution

---

[12] Although there have been several amendments to the federal statutes, commonly referred to as the Electronic Communications Privacy Act ("ECPA"), the original act was passed over twenty-five years ago in 1986.

In the intervening years, Congress considered overhauling the ECPA a number of times. On August 2, 2012, two congressmen introduced The Electronic Communications Privacy Act Modernization Act of 2012. The proposal is designed to "both protect the privacy of the information transmitted by digital communications and provide clear standards to guide law enforcement and the courts." *Nadler, Conyers Propose Critical Reforms to Cloud Computing Privacy Laws*, JERROLD NADLER (Aug. 2, 2012), http://nadler.house.gov/press-release/nadler-conyers-propose-critical-reforms-cloud-computing-privacy-laws. The bill would:

> [• R]equire the government to obtain a probable cause search warrant anytime it compels the contents of wire or electronic communications[;] . . .
> • Provide a uniform standard and set notice rules when the government accesses the contents of communications;
> • Amend the law to provide the same statutory suppression remedies for electronic communications as are currently provided for wire and oral communication surveillance[; and]
> • Add new – and, in some instances, modify existing – reporting requirements to ensure that Congress has sufficient information for effective oversight and possible future reforms.

Id. The August 2012 bill followed various attempts in Congress to amend the federal statutes, including hearings. *See ECPA Reform and the Revolution in Cloud Computing: Hearing before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Committee on the Judiciary*, 111th Cong. (2010), *available at* http://judiciary.house.gov/hearings/printers/111th/111-149_58409.PDF.

[13] One reason for this judicial reluctance may be that many judges may feel out of their depth because they lack much technological savvy. One commentator, for example, feels that the justices on the United States Supreme Court will find a search violative of the Fourth Amendment if "the justices could imagine [the incident] happening to them." Erwin Chemerinsky, *The Court and the Fourth Amendment: The Justices tend to find a violation if they can imagine the search applying to them personally*, NAT'L L.J., May 7, 2012, at 51. This uncomfortable feeling on the part of the Court to entangling itself in technology was obvious in *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2629, 2630 (2010). *See infra* notes 113-16 and accompanying text. For a discussion of *Quon*, *see infra* notes 151-55.

proposed in this paper is to be aware of the slight protection afforded by the statutes and the judiciary,[14] be proactive in learning how communication may be intercepted,[15]and take countermeasures to avoid someone surreptitiously monitoring our communication.[16]

Section II discusses examples of technology that have eroded privacy and Section III identifies privacy currently provided under statutes and case law. Section III analyzes privacy erosion through the lenses of the domino effect, the right to privacy, and the bad man. Finally, Section IV furnishes some solutions to the loss of privacy through technology.

II. EXAMPLES OF TECHNOLOGY THAT HAVE ERODED PRIVACY

This section discusses three examples of technology that have eroded privacy. They are the use of cell phones as microphones, key logger software, and packet sniffer software that captures Wi-Fi data.

A. CELL PHONE AS MICROPHONE

Prevalence of cell phone use is growing, and, because of this use of the cell phone, others are able to monitor a person's activities and may be able to listen in on our conversations. It may be wise to avoid discussing sensitive matters via cell phone and to refrain from leaving your cell phone unattended. These precautions are recommended because technology is available that allows the cell phone microphone to be remotely activated to capture conversations held in the vicinity of the phone.[17] Although one would love to know how this is accomplished, the method for remotely activating the cell phone microphone is "sketchy"[18] and not generally accessible by the layperson.

A number of companies claim that their software has this ability, with the software widely available on the Internet. The vendors place the onus on the consumer to comply with applicable law through an indirect[19] or more direct[20] legal

[14] *See infra* notes 35-112 and accompanying text.
[15] *See infra* notes 17-34 and accompanying text.
[16] *See infra* notes 150-60 and accompanying text.
[17] Eric Bland, *Malicious Software Turns Your Cell Phone Against You*, DISCOVERY NEWS (Mar. 9, 2010), http://news.discovery.com/tech/cell-phone-malware.html.
[18]Bruce Schneier, *Remotely Eavesdropping on Cell Phone Microphones*, SCHNEIER ON SECURITY (Dec. 5, 2006), http://www.schneier.com/blog/archives/2006/12/remotely_eavesd_1.html.
[19] For example, one website states:

> It is the responsibility of the end user to comply with all federal and state laws. Spy software will allow you to monitor mobile phones as a tool NOT for illegal purposes. Use at your discretion. It is a federal and state offense to install surveillance software onto a phone which you do not have proper authorization. We absolutely do not condone the use of our software for illegal purposes. The use of

> the software is done at your own discretion and risk and with agreement that you will be solely responsible for any damage to your mobile or loss of data that results from such activities. No advice or information, whether oral or written, obtained by you from us or from the Highster Mobile web site shall create any warranty for the software. In addition, you agree to hold harmless the publisher and authors personally and collectively for any losses of relationships, capital (if any) that may result from the use of this application. Your use of software obtained through or from CTS Technologies Corp. like other software agreements, indicates your acceptance of these disclaimers.

HIGHSTER MOBILE, http://www.highstermobile.com/ (last visited Aug. 2, 2012). Another states:

> Disclaimer: SpyBubble is a software program designed to gather information about a phone. You should be the legal owner of the phone or have permission from the user of the phone in order to install SpyBubble on it.
>
> If you don't comply with this, you may be breaking federal, state, or local laws, depending on where you live. User discretion and judgment is advised. By getting SpyBubble, you agree to use it for legal purposes only. You also agree to use the software at your sole discretion and responsibility, releasing SpyBubble from any legal responsibilities that result from your actions, including but not limited to loss of data and damage of equipment, as well as any legal consequences of your actions. Nothing explicit or implicit in this website will create a guarantee of any kind. (what about the 60 days guarantee?). In addition, you also agree to release the SpyBubble team as individuals or as a company from any legal responsibility resulting from any damage in relationships or loss of capital that may be caused from the use of the software. The use of SpyBubble will be taken as acceptance of this disclaimer.

SPY BUBBLE, http://www.spybubble.com/ (last visited Aug. 2, 2012).

[20] Another company includes legal terms that can be accessed at the bottom of the website's lengthy home page. The legal terms provide:

> **It is a federal and state offense to install surveillance software onto a phone which you do not have proper authorization.**
>
> We absolutely do not condone the use of our software for illegal purposes. In order to register you MUST agree to the following conditions.
>
> 1. You acknowledge and agree that you own the mobile phone you will install the software onto OR that you have the expressed written consent of the owner to be an authorized administrator of the phone and its users.
>
> 2. If you install our software onto a phone which you do not own or have proper consent, we will cooperate with law officials to the fullest extent possible. This includes turning over requested customer data, and any other purchase/product related information.
>
> 3. You agree that you will check all local, state and federal laws to make sure you are complying with all laws in your region. It may be illegal in your region to monitor other individuals on your own device. You will never monitor any adult without their valid permission.

notice. This type of software allowed the FBI to use a "roving bug" that "functioned whether the phone was powered on or off, intercepting conversations within its range wherever it happened to be."[21]

B. SOFTWARE THAT CAPTURES KEY STROKES

Software is readily available that logs key strokes input on a computer and that can be installed remotely. This means that someone can use the key logger software to monitor a target's computer use and to capture personal information such as a password, bank account number, social security number, or other sensitive information typically input into a computer with key strokes.

One version of the key logger software, RemoteSpy, was the subject of Federal Trade Commission action.[22] CyberSpy, the company selling RemoteSpy, claimed that legitimate uses for the software were to monitor online activities of a child or employee. Apparently, a lightning rod for the FTC was the fact that "RemoteSpy customers were given detailed instructions on how to disguise the spyware as an innocuous file—such as a photo—that could be attached to an email. When the file was opened, the keylogger software would be secretly installed."[23] Although still offered for sale online, the online marketing information for RemoteSpy was apparently revised to delete the offending instruction and wording was added specifying that the person attempting to install the key logger software must either own the computer on which the software is being installed or have consent from the computer owner.[24]

Similarly, cell phone software can secretly log key strokes, leading to a loss of privacy for the cell phone user's text messages, bank account numbers, passwords,

---

> 4. You agree that we are not liable for any type of damage, litigation, or legal predicaments that may arise due to use or abuse of any our products.

EASYSPY, http://www.spyanycellphone.info/legal-terms.php (last visited Aug. 2, 2012).

[21] *United States v. Tomero*, 462 F. Supp. 2d 565, 567 (S.D.N.Y. 2006). Although the FBI secured the requisite warrants prior to using the software, other law enforcement agencies may be tempted to use this technology to target business owners, among others, without first obtaining a court order.

[22] Amy L. Edwards, *Feds sue Orlando firm over 'spyware*,' ORLANDO SENTINEL, Nov. 21, 2009, at A1; *also see* F.T.C. v. Cyberspy Software, LLC, No. 6:08-cv-1872-Orl-31GJK (M.D. Fla. Nov. 25, 2008)(order granting preliminary injunction).

[23] Edwards, *supra* note 22.

[24] REMOTESPY, http://www.remotespy.com/howitworks.php (last visited Aug. 2, 2012). The explanation of RemoteSpy provides in part:

> [S]o long as the computer being monitored is owned by you (or you have written consent of the computer's owner), then you have the right to install any software you want onto that computer. If you do not own the computer being monitored or do not have written permission to monitor it, then you simply cannot use RemoteSpy. Such an unauthorized use would be a violation of the license agreement and, very possibly, against the law.

Id.

and other sensitive information. In November of 2011, Trevor Eckhardt, a security researcher, posted the allegation that software manufactured by Carrier IQ Inc. ("Carrier IQ"), a mobile analytics software company, was installed on the cell phones of a number of cell phone manufacturers, and surreptitiously recorded this information.[25] A number of cell phone users sued Carrier IQ for its alleged violation of federal wiretap statutes.[26] Carrier IQ called the software a diagnostic tool and disputed the claim that the software functioned to log key strokes.[27]

C. INTERCEPTION OF WI-FI DATA

Most businesses, and many homes, maintain their own Wi-Fi networks that are used to gather information, communicate, and transmit sensitive information, such as login information, bank account numbers, and security codes. In 2007, Google, Inc. began using Google Street View vehicles to photograph views of the streets travelled by the vehicles. These vehicles allegedly contained packet sniffer software with the ability to intercept data packets from various Wi-Fi networks the vehicles passed as they roamed the country's streets.[28] In response to a European privacy authority, Google, Inc. admitted that its vehicles had collected Wi-Fi data.[29] The alleged purpose of collection of the data was to improve Google, Inc.'s search and map services.[30] Various citizens filed a class action lawsuit against Google, Inc. claiming that the interception violated the federal wiretapping statutes.[31]

After capturing the data packets, the Google sniffer software "decodes or decrypts the data packet and analyzes the contents."[32] The decoding and analysis requires special processing of the data packets because "the data packets are not readable by the general public absent . . . sophisticated decoding and processing technology."[33] The lawsuit further explains that "to view the contents of the data packets captured by the wireless sniffer in a readable form, the packets must be

---

[25] Marcia Hofmann, *Carrier IQ Tries to Censor Research With Baseless Legal Threat*, ELECTRONIC FRONTIER FOUNDATION (Nov. 21, 2011), https://www.eff.org/deeplinks/2011/11/carrieriq-censor-research-baseless-legal-threat. The Trevor Eckhart November 28, 2011 video in which he demonstrates evidence of the key logging feature of Carrier IQ software can be found at https://www.youtube.com/watch?v=T17XQI_AYNo (last visited Aug. 5, 2012).

[26] *Leong v. Carrier IQ Inc.*, Nos. CV 12–01562 GAF (MRWx), CV 12–01564 GAF (MRWx)(C.D. Cal. April 27, 2012)(class action lawsuit); In re: Carrier IQ, Inc. Consumer Privacy Litigation, MDL No. 2330 (U.S. Jud. Pan. Mult. Lit. Apr. 16, 2012)(multidistrict litigation).

[27] Amanda Bronstad, *Suits accuse cell carriers of spying: Tracking software is said to violate Federal Wiretap Act*, NAT'L L.J., May 21, 2012, at 1. The information collected by the software appears to be dependent on its architecture. Peter Eckersley, *Some Facts About Carrier IQ*, ELECTRONIC FRONTIER FOUNDATION (Dec. 13, 2011), *https://www.eff.org/deeplinks/2011/12/carrier-iq-architecture.*

[28] *In re Google Inc. Street View Electronic Communications Litigation,* 794 F.Supp.2d 1067, 1070-71 (N.D. Cal. 2011).

[29] *Id.* at 1071.

[30] *Id.*

[31] *Id.* at 1070.

[32] *Id.* at 1071.

[33] *Id.*

stored on digital media and then decoded using crypto-analysis or a similarly complicated technology."[34]

III. PRIVACY PROTECTION UNDER FEDERAL AND STATE STATUTES AND CASE LAW

A reasonable expectation would be that communications are protected against interception by statutes and case law. This section examines the privacy provided under federal and state statutes and case law.

A. FEDERAL AND STATE STATUTES

The Electronic Communications Privacy Act ("ECPA")[35] protects face-to-face conversations, telephone conversations, and digital transfer of data by making it illegal to secretly access such communication. In addition, the Stored Communications Act ("SCA")[36] protects stored digital data to some degree. As explained below, state statutes also protect face-to-face conversations, telephone conversations, and digital transfer of data.

Under the ECPA, a face-to-face conversation receives protection so long as it qualifies as an "oral communication." For a conversation to satisfy the ECPA's oral communication criteria, the speaker must believe that the conversation is private and this belief must be reasonable.[37] A telephone conversation may be protected as a "wire communication" if it is audible by the human ear.[38] Digital information, such as computer data, may be protected as an "electronic communication."[39]

---

[34] *Id.*

[35] 18 U.S.C.A. §§ 2510-2522 (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)). Over the years, there have been a number of attempts to overhaul the ECPA. *See supra* note 12 and accompanying text.

[36] 18 U.S.C.A. §§ 2701-2712 (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)).

[37] Title 18 U.S.C.A. § 2510(2) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)) provides that "'oral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."

[38] Title 18 U.S.C.A. § 2510(1) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)) provides that a

> "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

[39] Title 18 U.S.C.A. § 2510(12) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)) provides that an "'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,

The ECPA makes it illegal for someone to deliberately intercept an oral, wire, or electronic communication. In addition, it is illegal for someone to deliberately disclose or use an illegally intercepted communication if the person knows or had reason to know that the oral, wire, or electronic communication has been illegally intercepted.[40] An exception exists if the action is taken with the consent of at least one party to the conversation so long as the purpose of the taping is other than to commit a crime or tort.[41] Another exception allows an employee of a wire or electronic communication service provider to intercept, disclose, or use a communication in the normal course of employment.[42] An illegally obtained oral or wire communication must be excluded from evidence. However, there is no similar exclusion for an illegally obtained electronic communication.[43]

The "aggrieved person,"[44] whose oral, wire, or electronic communication has been illegally intercepted, disclosed, or used, has a civil remedy against the one committing the illegal action.[45] The aggrieved person may obtain statutory damages

---

electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include . . . any wire or oral communication."

[40] 18 U.S.C.A. § 2511(1) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)).

[41] 18 U.S.C.A. § 2511(2)(d) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)). That sub-subsection provides:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

Id.

[42] 18 U.S.C.A. § 2511(2)(a)(i) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)). The statute provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

Id. This exception appears to be narrower than the exceptions under the Stored Communications Act. *Cf.* 18 U.S.C.A. §§ 2701(c), 2702(b) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)).

[43] 18 U.S.C.A. § 2515 (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)).

[44] 18 U.S.C.A. § 2510(11) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)).

[45] 18 U.S.C.A. § 2520(a) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)).

of the greater of actual damages or $100 per day, to a maximum of $10,000 and punitive damages. Other available relief includes preliminary injunctions, other equitable relief, declaratory relief, attorneys' fees, and costs.[46]

The SCA prohibits the deliberate accessing of an electronic communication service facility[47] and prohibits an entity providing electronic communication service or remote computing service from disclosing an electronic communication in storage.[48] Exceptions allow access by one providing the wire or electronic communication service, the service provider,[49] and disclosure to the addressee or intended recipient, or with the consent of the originator, the addressee, or the intended recipient, or to an employee.[50] One whose stored electronic communication has been illegally accessed has a civil remedy against the one committing the illegal action.[51] The aggrieved person may obtain actual damages plus profits obtained by the violator, with a minimum of $1,000, and punitive damages. Other relief includes preliminary injunctions, other equitable relief, declaratory relief, attorneys' fees, and costs.[52]

A person whose digital communication has been secretly accessed would attempt to claim that the communication is an electronic communication under the ECPA rather than an electronic communication under the SCA. There are two reasons for trying to seek relief under the ECPA rather than the SCA. The first reason is that the civil damages award is potentially higher under the ECPA than the SCA.[53] The second reason is that the exception for a service provider, which would allow the service provider to access digital communication without violation of federal statute, appears to be narrower under the ECPA than the SCA.[54]

All states but one, Vermont, have statutes that protect face-to-face conversations, telephone conversations, and electronic data against unauthorized access or disclosure. Many state statutes, like the federal statutes, allow access with the consent of one party and are similar to the federal statutes. A minority of the states allow access only upon consent of all parties. These minority, all-party

---

[46] 18 U.S.C.A. § 2520(b)-(c) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)).
[47] 18 U.S.C.A. § 2701(a) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)).
[48] 18 U.S.C.A. § 2702(a) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)).
[49] 18 U.S.C.A. § 2701(c) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)) provides: "Subsection (a) of this section does not apply with respect to conduct authorized--(1) by the person or entity providing a wire or electronic communications service." This exception appears to be broader than that available under the ECPA. *Cf.* 18 U.S.C.A. § 2511(2)(a)(i) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)).
[50] 18 U.S.C.A. § 2702(b) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)).
[51] 18 U.S.C.A. § 2707(a) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)).
[52] 18 U.S.C.A. § 2707(b)-(c) (West, Westlaw through P.L. 112-142 (excluding P.L. 112-140 and 112-141)).
[53] 18 U.S.C.A. § 2520(b)-(c) & § 2707(b)-(c). *See supra* notes 46, 52 and accompanying text.
[54] 18 U.S.C.A. § 2511(2)(a)(i) & § 2701(c). *See supra* notes 42, 49 and accompanying text.

consent states are California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Montana, New Hampshire, Pennsylvania, and Washington.[55]

B. APPLICATION OF STATUTES TO ACTIVATING A CELL PHONE FOR USE AS A MICROPHONE

Given that the technology is readily available, a layperson may not realize that using a cell phone as a microphone is illegal without at least one person's consent under the ECPA and in the majority of the states. As stated above, the minority of states require all parties' consent prior to someone intercepting a conversation. Using a cell phone as a microphone without the requisite consent to capture a telephone conversation is a violation of wiretapping statutes. Capturing a face-to-face conversation may be in violation of eavesdropping statutes if the persons whose conversation is being overheard are in a location where they expect privacy and that expectation is reasonable.

Although civil remedies are available to anyone whose telephone conversation or private in-person conversation has been intercepted, the person whose phone has been used as a microphone might never discover the interception. In contrast, the government is required to provide notice of the interception, so the person whose phone has been intercepted would discover the interception. There is a time limit on a government court order to intercept a conversation and the basis for obtaining a court order is scrutinized by a judge. However, there is no such oversight when a layperson intercepts.

C. PROTECTION AFFORDED ELECTRONIC DATA CAPTURED BY KEY LOGGER SOFTWARE

It might be reasonable to believe that the federal statutes would protect someone whose key strokes had been surreptitiously captured via a key logger software program. The courts, however, have interpreted the federal statutes narrowly, in a hyper-technical manner, finding that use of a key logger software program does not fall within the reach of the federal statutes. These courts looked at whether the key logged information was transferred contemporaneously with its capture or whether the key logged information was within the chain of interstate commerce.[56]

---

[55] From reading its statute, Michigan would seem to be an all-party consent state; however, case law has interpreted Michigan's wiretapping statute to allow surreptitious taping upon one-party consent. The theory behind this case law interpretation is that a party cannot "intercept" the party's own conversation. Bast, *supra* note 55 at 878-81. Although the Connecticut statutes allow one party to a face-to-face conversation to surreptitiously tape the conversation, the statutes require all-party consent to tape a telephone conversation. *Id*. at 927. In contrast, the Oregon statutes require all-party consent to tape an in-person conversation but allow one party to a telephone conversation to surreptitiously tape the conversation. *Id*. at 929.

[56] *See infra* notes 58-81 and accompanying text.

The first of the cases was decided in 2001 in *United States v. Scarfo*.[57] In *Scarfo*, the FBI was investigating Scarfo for alleged illegal gambling and loansharking when FBI agents used search warrants to search Scarfo's office, including his computer. The agents were unable to access a passphrase-protected encrypted file on Scarfo's computer. Pursuant to additional warrants, they returned, installed a key logger software program (KLS) on the computer, and used the software to capture the passphrase, thereby obtaining access to the file.[58]

The issue for the court was "whether the KLS intercepted a wire communication in violation of the wiretap statute by recording keystrokes of e-mail or other communications made over a telephone or cable line while the modem operated."[59] The wording of the issue shows that the court would not consider the KLS to violate the ECPA unless the captured keystrokes were being transmitted contemporaneously with their input. This viewpoint is also reflected in the court's explanation of the operation of the KLS, "[r]ecognizing that Scarfo's computer had a modem and thus was capable of transmitting electronic communications via the modem, the F.B.I. configured the KLS to avoid intercepting electronic communications typed on the keyboard and simultaneously transmitted in real time via the communication ports."[60] The court held that the FBI's use of the KLS had not violated the ECPA and denied Scarfo's motion to suppress.[61]

United States v. Ropp,[62] decided in 2004, is another case that addresses this issue. Ropp installed a key logger program on an insurance company computer that captured key strokes being transmitted between the keyboard and the central processing unit.[63] The court focused on the "affect[ing] interstate . . . commerce" portion of the definition of electronic communication and stated the issue as "whether internal computer transmissions can be viewed as transmissions by a

---

[57] *United States v. Scarfo*, 180 F. Supp. 2d 572 (D. N.J. 2001). "This case presents an interesting issue of first impression dealing with the ever-present tension between individual privacy and liberty rights and law enforcement's use of new and advanced technology to vigorously investigate criminal activity." *Id.* at 574.

[58] *Id.*

[59] *Id.* at 581.

[60] *Id.* at 581-82. The FBI expert explained:

> The default status of the keystroke component was set so that, on entry, a keystroke was normally *not* recorded. Upon entry or selection of a keyboard key by a user, the KLS checked the status of each communication port installed on the computer, and, all communication ports indicated inactivity, meaning that the modem was not using any port at that time, then the keystroke in question would be recorded.

Id. at 582.

[61] *Id.*

[62] *United States v. Ropp*, 347 F. Supp 2d 831 (C.D. Cal. 2004).

[63] *Id.* at 831. The reported case does not disclose how Ropp's actions were discovered nor why the government decided to prosecute.

system that affects interstate commerce to determine whether they constitute 'electronic communications' under the Wiretap Act."[64] In reaching its holding, the court relied on *Scarfo* and the panel decision in *United States v. Councilman*. After *Ropp* was decided, the United States Court of Appeals for the First Circuit reconsidered *Councilman* en banc and reversed.[65] Thus, the *Ropp* court did not have the benefit of the First Circuit en banc opinion in reaching its decision.

The *Ropp* court held that "the communication in question is not an 'electronic communication' within the meaning of the statute because it is not transmitted by a system that affects interstate or foreign commerce."[66] The court reasoned that "[t]he network connection is irrelevant to the transmissions, which could have been made on a stand-alone computer that had no link at all to the internet or any other external network."[67] The court recognized that although this was a "gross invasion of privacy" it did not fall within the ECPA. It declined to interpret the statute more expansively suggesting that it is up to Congress to act.[68]

In *United States v. Barrington*,[69] three undergraduates at Florida A&M University implemented a scheme to install key logger software on several university computers to capture usernames and passwords of authorized personnel working in the university registrar's office and transmit the information via email to Barrington and others. Barrington was convicted on five counts and sentenced to eighty-four months in prison and appealed.[70]

In considering whether his sentence was calculated correctly, the appellate court considered if the key logger capture of the usernames and passwords violated the ECPA. The court first explained that for an illegal interception to occur, the interception must be contemporaneous with the transmission of the electronic communication.[71] "Accordingly, use of a keylogger will not violate the Wiretap Act if the signal or information captured from the keystrokes is not at that time being transmitted beyond the computer on which the keylogger is installed (or being otherwise transmitted by a system that affects interstate commerce)."[72] The *Barrington* court found that the key logger software did not have that capability.[73] The appellate court affirmed Barrington's conviction and sentence.[74]

---

[64] *Id.* at 833.
[65] *United States v. Councilman*, 373 F.3d 197 (1st Cir. 2004), *rev'd*, 418 F.3d 67 (1st Cir. 2004)(en banc).
[66] *Ropp*, 347 F. Supp 2d at 837.
[67] *Id.* at 838.
[68] *Id.*
[69] *United States v. Barrington*, 648 F.3d 1178, 1184 (11th Cir. 2011).
[70] *Id.* at 1183.
[71] *Id.* at 1202.
[72] *Id.* The court followed *Scarfo* and *Ropp* in this interpretation of the ECPA. *Id.* at 1202 n.25.
[73] *Id.* at 1203.
[74] *Id.* at 1204.

In *Rene v. G.F. Fishers, Inc.*,[75] employees installed key logger software on the computer Rene used at work. The software captured the key strokes made on the computer and emailed the information to other employees from time to time. The other employees thus obtained Rene's email and personal checking account passwords and used them to access Rene's email and checking account. Rene's confrontation over other employees' access to her email and checking account led to her termination from employment based on trumped-up evidence of poor performance.[76]

Rene sued her former employer and former co-workers under the ECPA, the SCA, and the state wiretapping statute.[77] The court held that Rene's allegation that the other employees violated the ECPA failed because there was no interception under the statute.[78] The court followed the statutory interpretation of *Barrington* and *Ropp* that "while the Defendants' keylogger software may have captured transmissions in transit, the system through which these signals traveled did not affect interstate or foreign commerce."[79] The court allowed Rene's claim under the SCA to proceed. "By alleging that the Defendants made unauthorized access to her email, Rene has satisfied her burden of asserting a violation of the SCA."[80]

At least two courts have questioned, in passing, *Ropp's* overly-technical requirement that interception occur within the stream of interstate commerce rather than affecting interstate commerce. In *Potter v. Havlicek*, the court stated, "The [*Ropp*] decision, however, seems to read the statute as requiring the communication to be traveling in interstate commerce, rather than merely 'affecting' interstate commerce."[81] The *Potter* court added, "It seems to this Court that the keystrokes that send a message off into interstate commerce 'affect' interstate commerce."[82] The court in *Brahmana v. Lembo*[83] seemed to be favorably impressed by the *Potter* court reasoning: "*Ropp* reads the statute as requiring that the communication must be traveling in interstate commerce as opposed to merely 'affecting interstate commerce.' . . . The keystrokes, while not traveling in interstate commerce, do 'affect interstate commerce.'"[84]

As more fully explained above, most courts that have dealt with cases involving key logger software have taken a fairly narrow approach, finding that recording key strokes prior to transmission of information did not violate the ECPA

---

[75] *Rene v. G.F. Fishers, Inc.,* 817 F. Supp. 2d 1090, 1092 (S.D. Ind. 2011).
[76] *Id.*
[77] *Id.*
[78] *Id.* at 1094.
[79] *Id.*
[80] *Id.* at 1097.
[81] *Potter v. Havlicek*, No. 3:06-cv-211, 2007 WL 539534, at *8 (S.D.Ohio Feb. 14, 2007).
[82] *Id.*
[83] *Brahmana v. Lembo*, No. C-09-00106 RMW, 2009 WL 1424438 (N.D. Cal. May 20, 2009).
[84] *Id.* at 3.

either because the recording was not contemporaneous with information transfer or the recording did not affect interstate commerce. With this interpretation of the ECPA, a knowledgeable computer person as in *Scarfo*, can set up a key logger program either on a computer or on a cell phone to deftly navigate around the ECPA. This leaves some of one's most sensitive information, such as username, password, and bank account, ripe for the picking.

It will be interesting to observe how the court handling the Carrier IQ litigation applies the ECPA, whether the court follows the narrow approach of most of the courts or takes the lead in applying a more expansive interpretation of the ECPA.

D. PROTECTION ACCORDED INTERCEPTED EMAIL

Email messages can be routed to someone other than the intended recipient either by forwarding a copy of the email to a third party or by using spyware. The circuits to consider whether the ECPA has been violated have required that the email capture be contemporaneous with transmission. The courts have been fairly open to finding a violation of the ECPA even where the email may have been intercepted when in temporary storage or when a copy of an email is transmitted to a third party almost simultaneously with its transmission to the intended recipient.

In *United States v. Councilman*,[85] the defendant was vice-president of Interloc, Inc., an online rare book dealer. He managed the free email service offered to the company's customers. Councilman directed company employees to copy all emails to customers from Amazon.com and place them in a mailbox to which Councilman had access.[86] This interception of customer emails led to an indictment alleging Councilman's conspiracy to violate the ECPA.[87]

The issue before the United States Court of Appeals for the First Circuit, en banc, was "whether interception of an e-mail message in temporary, transient electronic storage states an offense under the Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522."[88] The court held "that the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process for such communications."[89] The court reasoned, "we doubt that Congress contemplated the existential oddity that Councilman's interpretation creates: messages—conceded by stipulation to be

---

[85] *United States v. Councilman*, 418 F.3d 67, 70 (1st Cir. 2005)(en banc).
[86] *Id.*
[87] *Id.* at 71.
[88] *Id.* at 69. The en banc decision followed the trial court dismissing the indictment and a divided First Circuit panel affirming. *Id.* The case provides a helpful description of the manner in which email is transmitted. *Id.* at 69-70.
[89] *Id.* at 79.

electronic communications—briefly cease to be electronic communications for very short intervals, and then suddenly become electronic communications again."[90]

In *United States v. Szymuszkiewicz*,[91] the United States Court of Appeals for the Seventh Circuit was confronted by similar facts and reached a decision similar to the decision in *Councilman*. IRS employee, Szymuszkiewicz, monitored his supervisor's email correspondence by having a copy of her incoming emails forwarded to him. A setting on the supervisor's Microsoft Outlook email program forwarded all of the supervisor's emails to Szymuszkiewicz. He was convicted under the ECPA of deliberately intercepting his supervisor's emails.[92]

The court found that the IRS regional server in Kansas City sent two copies of the email intended for the supervisor, with one to the supervisor and one to Szymuszkiewicz. Thus, the interception of the email was contemporaneous with the email transmission, [93] as required by several judicial circuits that have considered the elements necessary for the interception of an electronic communication to violate the ECPA.[94] The appellate court affirmed the conviction.[95]

Another method of monitoring someone's electronic activity is through the installation of spyware. In *Klumb v. Goan*,[96] Crystal Goan installed spyware on a computer Roy Klumb, her husband, used at work. The spyware captured key strokes, recorded websites visited and applications used, took screenshots of instant messages, forwarded copies of incoming email messages and instant messages in progress, and reported recorded information to a specified email address.[97] Klumb sued his then ex-wife, Goan, alleging that her use of spyware violated the ECPA and the SCA.[98]

The court found that Goan had violated the ECPA.[99] Goan "via eBlaster [spyware] intentionally and automatically intercepted emails sent to plaintiff through the internet and forwarded copies to herself through the internet at cmgoan@yahoo.com when plaintiff opened those emails for the first time from the Dell or Vista computer."[100] The court followed the reasoning of the court in

---

[90] *Id.* at 78.
[91] *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010).
[92] *Id.* at 703. The case provides a helpful description of the manner in which email is transmitted. *Id.* at 704-05.
[93] *Id.* at 704, 705-06.
[94] *See Fraser v. Nationwide Mutual Insurance Co*., 352 F.3d 107, 113 (3d Cir. 2003); Steve Jackson Games, Inc. v. Secret Service, 36 F.3d 457, 460-61 (5th Cir. 1994); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002); *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003).
[95] *Szymuszkiewicz*, 622 F.3d at 707.
[96] *Klumb v. Goan*, No. 2:09–cv–115, 2012 WL 2958228 (E.D.Tenn. July 19, 2012).
[97] *Id.* at 3.
[98] *Id.* at 1.
[99] *Id.*
[100] *Id.* at 15.

Szymuszkiewicz and explained that "under the router switching analysis, a wiretap occurs when spyware automatically routes a copy of an email, which is sent through the internet, back through the internet to a third party's email address when the intended recipient opens the email for the first time."[101] The court did not believe Goan's defense that she had Klumb's consent to install the spyware on the computer he used.[102] The court awarded Klumb $10,000 in statutory damages and $10,000 in punitive damages for Goan's "outrageous and egregious conduct," and found that Klumb was entitled to reasonable attorney's fees and costs.[103]

Shefts v. Petrakis[104] also involved the use of spyware installed to record Shefts' emails and text messages. Shefts, Petrakis, and two others were officers and directors of a business.[105] Shortly following the installation of the spyware, the directors approved an employee manual placing employees on notice that the business had the right to monitor electronic communication on business equipment.[106] "The Company . . . reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use of the Internet and of computer equipment used to create, view, or access e-mail and Internet content."[107] The employee manual further provided: "Employees must be aware that the electronic mail messages sent and received on Company equipment are not private and are subject to viewing, downloading . . . and archiving by Company officials at all times."[108]

The court had to determine whether Shefts' motion for summary judgment should be granted for the defendants' violating the ECPA by intercepting Shefts' text messages. The court found that the text messages had been intercepted, but that the court would not grant the motion for summary judgment because Shefts consented to the interception;[109] Shefts had knowledge of the server capability and the employee manual made it clear that electronic communication was subject to archiving.[110] Similarly, the court denied Shefts' motion for summary judgment for defendants' violation of the SCA, finding that the monitoring of Shefts' text messages and emails was consensual.[111]

---

[101] *Id.*
[102] *Id.* at 16.
[103] *Id.* at 20.
[104] *Shefts v. Petrakis*, 758 F. Supp. 2d 620 (C.D. Ill. 2010).
[105] *Id.* at 625.
[106] *Id.* at 625-26.
[107] *Id.* at 626.
[108] *Id.* at 631.
[109] *Id.* at 629-30.
[110] *Id.* at 630-31. Shefts' intercepted email messages were not the subject of a motion for summary judgment; however, had they been, the court presumably would have reached the same conclusion with respect to the intercepted emails as it did for the intercepted text messages.
[111] *Id.* at 635.

With the quantity of information transmitted via email, someone who intercepts a target's email traffic either by having a copy of each email forwarded or by using spyware may be able to read the target like an open book. It is fortunate for the target that the courts considering these cases have largely taken a broader view of the concept of interception to include an email while in temporary storage and a forwarded email.

Although the United States Court of Appeals for the First Circuit in *Councilman* needed the case to be considered en banc, that court took the lead in a well-reasoned decision that was followed by the United States Court of Appeals for the Seventh Circuit in *Szymuszkiewicz*. These two decisions provide some protection for emails given the existent email technology.

IV. ANALYSIS

This section provides some analysis of the current erosion of privacy by technology. The section first introduces the "domino effect" of court decisions and then examines privacy erosion via the right to privacy and the bad man.

A. THE DOMINO EFFECT

With the rapid advances in technology, a court is understandably reluctant to be the one to decide a case of first impression, as was the United States Supreme Court in *City of Ontario v. Quon*[112] in its 2010 decision. In an unusual step, the United States Supreme Court in *Quon* stated its reticence to reach too far. "The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[113] So as not to be misunderstood, the Court cautioned the reader, "[p]rudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices."[114] Then, the Court cautioned the reader again, "[a] broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds."[115]

---

[112] *City of Ontario v. Quon*, 130 S. Ct. 2619, 2629 (2010). For a discussion of *Quon*, *see infra* notes 151-54.

[113] *Id.* at 2629. This statement perhaps ironically gives a glimpse of the Court's slight passing familiarity with digital technology. The technology being considered was the pager, considered by most to be retro and, therefore, it is unlikely that the role of the pager is going to become any clearer.

[114] *Id.*

[115] *Id.* at 2630.

The burden of deciding a case involving technology may be a little lighter on a court's shoulders if the court can follow a pathway blazed by another court, even if the weight of the earlier court's decision is only one of persuasive authority.[116] A court following established precedent may be more comfortable than if it were the one to potentially set the course of the law on a controversial issue; thus, being in conformity with the earlier decision gives the court reaching the later decision some confidence that it is reaching the right decision. As more courts follow the initial decision, a later court may feel (vocab.) to rule contrary to an established line of cases.

This phenomenon is illustrated by the key logger software cases discussed above. *Scarfo*, the first in a line of cases, found that use of the key logger software had not violated the ECPA because the software was not capturing information while in transit. *Ropp*, the second case, relied on *Scarfo*; *Barrington*, the third case, cited to *Scarfo* and *Ropp*; and *Rene*, the fourth case, followed *Barrington* and *Ropp*. Did the first decision, *Scarfo*, correctly interpret the statute, given that there is a tendency for courts not to stray from what other courts have done?

The path of the common law can be analogized to the domino effect observable in a common childhood activity. A row of dominos might be set up on the floor of a room in an elaborate pattern. Once the pattern is completed, the first domino can be tipped into its neighboring domino, which very quickly leads to a toppling of all the dominos in the room; the more study and planning involved in setting up the dominos, perhaps the better the result will be. This more spectacular display may be similar to a well-reasoned court decision interpreting a statute that takes into account the broad legislative intent of the statutory scheme and reaches the result that the legislature would have chosen, had the legislature been confronted with the facts involving a new technology. However, what if in the middle of setting up the dominos, the person's hand slips, setting off a chain reaction? In that circumstance, it is impossible to stop the succeeding dominos from falling, and the result perhaps is not the best or what was ultimately intended by the legislature.

How does the domino effect apply to the above decisions, and which of the two domino effects (vocab – are applicable)? An ill-executed domino effect can be noted in several of the communication decisions that are narrow in effect. One example is the requirement that, for a violation of the ECPA, the interception must be contemporaneous with the email transmission.[117] Another example is that the courts have found that key logger software that logged key strokes pre-transit did not

---

[116] An exception to this follow-the-leader behavior might be a decision from a court perceived to be an outlier, such as a decision from a California court well-known to be liberal.

[117] *See Fraser v. Nationwide Mutual Insurance Co*., 352 F.3d 107, 113 (3d Cir. 2003); *Steve Jackson Games, Inc. v. Secret Service*, 36 F.3d 457, 460-61 (5th Cir. 1994); *Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868, 878 (9th Cir. 2002); *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003).

violate the ECPA.[118] In contrast, two circuit courts were open to finding a violation of the ECPA even where the email may have been intercepted when in temporary storage or when a copy of an email is transmitted to a third party almost simultaneously with its transmission to the intended recipient.[119]

B. BRANDEIS' RIGHT TO PRIVACY AND HOLMES' BAD MAN

Louis D. Brandeis and Oliver Wendell Holmes, contemporaries on the United States Supreme Court, were both eminent jurists and authors whose writings influenced the course of the law. Brandeis' views on privacy and Holmes' intriguing invitation to view the law from the prospective of the bad man, offer some insight into the present technological threats to communication privacy.

In 1890, Brandeis and his partner, Samuel D. Warren, spurred the creation of a new tort for invasion of privacy with their law review article, *The Right to Privacy.*[120] In the article they highlighted the importance of communication privacy to the individual's wellbeing and the detrimental effect that technological advances have had, and would continue to have, on privacy. They viewed communication privacy as fundamental. "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[121] Although they were largely concerned by the ability of the photographer to invade one's privacy, their discussion of the pernicious effect of technology was prescient of what was to come and sounds quite modern in tone. "Recent inventions and business methods . . . have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[122] A new technology (vocab – "that was emerging")at the time the article was being written enables sound recording. "[T]he existing law affords a principle which may be invoked to protect the privacy of the individual from invasion . . . by . . . the possessor of any other modern device for recording or reproducing scenes or sounds."[123]

The tension we feel today between conserving our communication privacy in the face of steadily advancing technology is analogous to that of the 1890s with the authors' expressing concern over the publication of photographs without the subject's consent in the newspaper; this was seen as violating the individual's

---

[118] *Rene v. G.F. Fishers, Inc*., 817 F. Supp. 2d 1090, 1094 (S.D. Ind. 2011); *United States v. Barrington*, 648 F.3d 1178, 1202 (11th Cir. 2011); *United States v. Ropp*, 347 F. Supp 2d 831, 838 (C.D. Cal. 2004); *United States v. Scarfo*, 180 F. Supp. 2d 572, 582 (D. N.J. 2001).

[119] *United States v. Szymuszkiewicz*, 622 F.3d 701, 704, 705-06 (7th Cir. 2010); *United States v. Councilman*, 418 F.3d 67, 78-79 (1st Cir. 2005)(en banc).

[120] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[121] *Id.* at 198.

[122] *Id.*

[123] *Id.* at 206.

personality.[124] They suggested a new legal principle under which the individual is provided a right "to be let alone,"[125] with the law safeguarding the "inviolate personality."[126] The authors envisioned this right to privacy "as a more general right to the immunity of the person, -- the right to one's personality."[127] This new legal principle was necessary to protect the individual's privacy from intrusion facilitated by advances in technology.[128]

Almost forty years later, Brandeis continued his concern for privacy in communication in his famous dissent in *Olmstead v. United States* In *Olmstead*, the federal government wiretapped eight telephones used by suspects over almost five months.[129] Brandeis warned that technology was providing an unfair advantage to the government. "Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."[130] In the future, technology would provide the government with ability far beyond wiretapping. "The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping."[131] He forecast that technology could lead to the government being able to surreptitiously invade even the inner recesses of the home. "Ways may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."[132] Echoing the idea from *The Right to Privacy* that the common law must evolve to meet changes in society,[133] Brandeis advocated that the Court expand its interpretation to find wiretapping a search and seizure under the Fourth Amendment. "Clauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world."[134]

In 1897, Oliver Wendell Holmes spoke of the "bad man" in his address, entitled *The Path of the Law*, upon the dedication of a new lecture hall at the Boston University School of Law.[135] Acknowledging that the law is "systematized prediction,"[136] Holmes distinguished for the audience the difference between the law,

---

[124] *Id.* at 195.
[125] *Id.* at 193, 205.
[126] *Id.* at 204, 205.
[127] *Id.* at 207.
[128] *Id.* at 208, 213.
[129] *Id.* at 471.
[130] *Id.* at 473.
[131] *Id.* at 474.
[132] *Id.*
[133] Warren & Brandeis, *supra* note 121 at 205. "Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society." *Id.* at 193.
[134] *Olmstead*, 277 U.S. at 471.
[135] Holmes, *supra* note 1 at 457, 457 n.1.
[136] *Id.* at 458.

which may have some impact on one not guided by moral principles, the bad man, and morality, which is based on ethical principles.[137]

> You can see very plainly that a bad man has as much reason as a good one for wishing to avoid an encounter with the public force, and therefore you can see the practical importance of the distinction between morality and law. A man who cares nothing for an ethical rule which is believed and practiced [sic] by his neighbors is likely nevertheless to care a good deal to avoid being made to pay money, and will want to keep out of jail if he can.[138]

In other words, one attempting to do what is right, may look beyond the law, while the bad man is risk adverse and acts to avoid some negative consequence that the law may impose. "But if we take the view of our friend the bad man we shall find that he does not care two straws for the axioms or deductions, but that he does want to know what the . . . courts are likely to do in fact."[139] Holmes queries, "But what does [legal duty] mean to a bad man?"[140] Then, to a bad man a legal duty is "a prophecy that if he does certain things he will be subjected to disagreeable consequences by way of imprisonment or compulsory payment of money."[141]

In protecting communication privacy in a technology-pervasive world, it would be well to keep in mind the bad man. Although the hope would be that the typical individual would respect another's privacy by not intercepting communication, this might not be the viewpoint held by competitors, thieves, and the curious, those who view the temptation to snoop on otherwise private communication too tempting to resist.

Combining the ideas of two great thinkers from the 1890's and the domino effect leads us to the realization that today's bad man, a competitor, a thief, or one with idle curiosity, has the ability to invade our communication privacy in ways alluded to by Brandeis but ones that he hardly could have imagined. Given the woeful protection provided much modern communication by the statutes and the courts, and the unlikelihood of the snooping being discovered or the snoop being caught, the bad man has full rein to pursue gathering our most vital information without our consent and the domino effect seems to be leading to a further toppling of privacy.

---

[137] *See* Holmes, *supra* note 1 and accompanying text.
[138] Holmes, *supra* note 1 at 459.
[139] *Id.* at 460.
[140] *Id.* at 461.
[141] *Id.*

For example, communication interception technology in China[142] and Russia[143] is so sophisticated that a business person traveling from the United States to one of these countries is well-advised to take certain measures to create a digital communication barrier when crossing the border into either country. The recommendation is to travel "electronically naked" by leaving one's personal cell phone and computer at home and using a new cell phone and computer while in the foreign country.[144] The cell phone should never be let out of one's sight and should be turned off when not in use, with the battery removed. Connection to the internet should be made only through an encrypted and password-protected route, with high security information, such as a password, copied from a thumb drive so as to refrain from using key strokes to input the information. These measures are to safeguard against a business competitor remotely activating the cell phone as a microphone, penetrating computer communication, or copying typed information via software that logs key strokes.[145] Without these measures, the business person runs the risk of unknowingly losing vital proprietary information to a competitor, with the loss perhaps only known in hindsight, a long time after the trip ended. Even worse, a nefarious person with company security information could remotely penetrate the company network.

Another point of vulnerability may be through the Federal Bureau of Investigation's Digital Collection System Network (DCSN), established as an outgrowth of 1994 federal legislation[146] mandating that telecommunications companies make their networks accessible to the federal government upon court order and thus giving the federal government access to telephone conversations and text messages. There may be similar switching points built into telecommunications

---

[142] One may not need to travel abroad to be vulnerable to foreign technology. For example, October 2011 and November 2011 reports chronicled Chinese government involvement in espionage. "Chinese actors are the world's most active and persistent perpetrators of economic espionage. US private sector firms and cybersecurity specialists have reported an onslaught of computer network intrusions that have originated in China, but the [Intelligence Community] cannot confirm who was responsible." OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, *supra* note 4. "In continuation of previous practice, China in 2011 conducted and supported a range of malicious cyber activities." U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, 2011 REPORT TO CONGRESS OF THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION 172 (2011), *available at* http://www.uscc.gov/annual_report/2011/annual_report_full_11.pdf. The report stated that "[t]hese included network exploitations to facilitate industrial espionage and the compromise of U.S. and foreign government computer systems." *Id.*

[143] Apparently, Russia is also conducting industrial espionage outside its borders. "Russia's intelligence services are conducting a range of activities to collect economic information and technology from US targets." OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, *supra* note 4.

[144] Nicole Perlroth, *Traveling Light in a Time of Digital Thievery*, N.Y. TIMES, Feb. 10, 2012, *available at* http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html?_r=1.

[145] *Id.*

[146] Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994)(codified at scattered sections of 18 U.S.C.).

networks allowing a telecommunications company employee or technologically-knowledgeable (vocab) outsider a back door into the telecommunications network. With this wiretap ability woven into the architecture of the telecommunications system, it is not inconceivable that a hacker could use the DCSN or similar access to a telecommunications company to spy on telephone conversations and text messages.[147]

V. SOLUTIONS TO VANISHING PRIVACY

A cynical person may take the attitude that perhaps the only way more privacy may be accorded to communication technology under the law is if a politician becomes an innocent target of an investigation. For example, in February 2012 the White House released a white paper, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*,[148] that has as its centerpiece *The Consumer Privacy Bill of Rights*, and calls on Congress to implement it by passing legislation.

However, given the delay in the history of enacting communication privacy legislation, it would be well to stem the tide by taking defensive measures to protect our communication privacy. Imagine a bad man surveying the communication landscape with the hope of finding someone whose communication privacy is easily penetrated. The bad man who finds someone whose privacy is fairly well protected because of defensive measures taken may move on to an easier target. This section describes defensive actions that one would be well-advised to take to safeguard one's communication privacy.

When dealing with highly sensitive information, a business person may be well-advised to adopt the measures of those visiting Russia or China. Given the availability of key logger software, it may make sense to copy a username, a password, and other similarly-sensitive information from a flash drive rather than input that information. A cell phone battery that is depleting rapidly may be an indication that the cell phone is activated as a microphone.

A 2010 United States Supreme Court case, *City of Ontario, Cal. v. Quon*,[149] highlights the lack of privacy the employee typically has while using employer-owned communication technology. In *Quon*, the government employer supplied text pagers to its police department SWAT team members, one of whom was Quon.[150]

---

[147] Ryan Singel, *Point, Click . . . Eavesdrop: How the FBI Wiretap New Operates*, WIRED, Aug. 29, 2007, http://www.wired.com/politics/security/news/2007/08/wiretap?currentPage=all. Such a breach occurred in Greece in 2005 through the Vodafone network. *Id.*

[148] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY i (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[149] *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010).

[150] *Id.* at 2624.

There was conflict between a computer policy, a privacy policy memorialized in a memo, and verbal directions from a department lieutenant, such that it was unclear whether Quon had a reasonable expectation of privacy in his text messages.[151] The Court assumed that Quon did have a reasonable expectation of privacy, but the Court found that the search was justified as work-related and as reasonable in scope.[152]

A solution to the vulnerability of the employee's personal communication is for the employee to obtain his or her own equipment. In *Quon*, the Court offered the following suggestion: "the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own."[153]

Another lesson from *Quon*, is that the employer should make sure that company policy on employee use of company-owned equipment specifies the use that the employee can make of the equipment and specifies whether the employer can monitor employee communications. If the company uses employee social-networking sites as a marketing tool, the policy should specify ownership of social networking accounts.[154] The policy should be updated regularly to cover new equipment and new technology, as well as data stored on the cloud.[155] Also, a lesson from *Quon* is that the employer should refrain from sending mixed signals, with the written policy differing from the oral policy or the policy applied in practice.

A business policy for companies retaining customer personal data is essential to ensure compliance with federal and state statutes that require those companies to safeguard such information and report theft of such information.[156] In addition (vocab – "for example), the Sarbanes-Oxley Act requires members of the New York Stock Exchange to have policies in place concerning their protection of personal and other critical data.[157]

A business should assess the risks that a bad man could pose to the company and continuously monitor its digital data and be cognizant of any security threats to that data. A basic measure is to develop a security plan for protecting company data that fits hand in glove with the company's business strategy. The security plan should be integrated into the business culture, rather than be a retrofit strategy more attuned to putting out fires. The plan should include human resource screening of employee applicants and employee training on appropriate protection

---

[151] *Id.* at 2625.
[152] *Id.* at 2630, 2631.
[153] *Id.* at 2630.
[154] Nick Akerman, *Company computer policies risk becoming obsolete: Policies must reflect new laws and court decisions on data theft, social networking and cloud computing*, NAT'L L.J., Apr. 2, 2012, at 47.
[155] *Id.*
[156] *Id.*
[157] *Id.*

and use of business data. Training might include common sense measures, such as being wary of what one clicks on in an email and not inserting a USB of unknown providence into one's computer.

One way to be proactive is to hire a technology security company to perform a security audit and implement suggested security measures. In the future, a company may retain a technology security company in the same way it retains an accountant and an attorney, with security audits performed on a regular basis.

Types of employer data should be reviewed and only by those with need to know access to the most sensitive data; this review should be done on a periodic basis. The employer can limit the personnel with access to sensitive information; require these personnel to keep logs of access with the employer monitoring the logs on a regular basis. Additional security measures may include protecting valuable information with two-factor authentication[158] that would require the user to produce something in addition to a password to access sensitive data.

The user of a subscription-based database should attempt to negotiate anonymity by having the service provider limit data collected and stored. A computer user accessing a free website should review the website's privacy policy; opt not to provide personal data; be cautious when linking from a search to a website; limit tracking tools by electing maximum privacy browser settings; and using software designed to make the internet user anonymous.

An email sender may be able to prevent internet service provider access to email content by encrypting email content. Simple measures, such as securing email and other accounts via password or two-factor authentication, resisting the temptation to share the password even with family members, changing passwords on a regular basis, and using different passwords for different accounts may provide some protection from the casual snoop.

VI. CONCLUSION

So—what can the bad man teach us about our privacy? One lesson is for us to critically examine the communications statutes as applied by the judiciary to determine what protection they afford. The lesson learned is that it is short-sighted to expect the law, as presently formulated, to protect our privacy; if we want to have privacy in communications we need to take offensive steps.

---

[158] Two-factor authentication would not allow the user access to a particular data base or piece of equipment unless the user provides at least two of three types of information. The first type is something the user knows (like a password), the second type is something the user possesses (like an ATM card or a token), and the third type is something the user is (like the recognition of the user via a biometric scan of the user's fingerprint or iris). *Two-factor authentication*, WIKIPEDIA, http://en.wikipedia.org/wiki/Two-factor_authentication (last visited Sept. 7, 2012).

Viewing privacy from the bad man's perspective is very useful in teaching us to acknowledge that there are gaps in statutory and judicial protection. These gaps, when combined with technology such as key logger software not to mention technological advances of the future, leave us vulnerable, as does our lack of knowledge that our communication has been intercepted through technology such as that which allows activation of a cell phone as a microphone.

Our loss of privacy is like Holmes' dragon, powerful but usually hidden. "When you get the dragon out of his cave on to the plain and in the daylight, you can count his teeth and claws, and see just what is his strength."[159] So—the bad man allows us to move the dragon, our loss of privacy, into plain view. "But to get him out is only the first step."[160] What is the next step? The next step is to take whatever offensive measures necessary to recoup our privacy. "The next is either to kill him, or to tame him and make him a useful animal."[161]

This article predicts the effect of the application of law and technology on communication privacy and discloses the risk that our communication will be open like a book because of increasingly sophisticated technology and the weakness of statutory and judicial protection. Thus, it is up to us, as risk avoiders, to take whatever steps necessary to regain communication privacy.

[159] Holmes, *supra* note 1 at 469.
[160] *Id.*
[161] *Id.*