Cornell Law Review

Volume 100
Issue 5 *July 2015*

Article 4

Cover your Webcam: The ECPA's Lack of Protection against Software That Could Be Watching You

Gariella E. Bensur

NOTE

COVER YOUR WEBCAM: THE ECPA'S LACK OF PROTECTION AGAINST SOFTWARE THAT COULD BE WATCHING YOU

Gabriella E. Bensur†

† B.A., Cornell University, 2012; J.D., Cornell Law School, 2015; Note Editor, *Cornell Law Review*, Volume 100. I would like to thank all of my family and friends who supported me and listened patiently while I discussed this Note and the Members of *Cornell Law Review* for all of their hard work.

INTRODUCTION

In July 2010, Crystal Byrd decided to lease and then purchase a laptop from a local rental company, Aspen Way, a franchisee of Aaron's Incorporated.[1] In December 2010, after Mrs. Byrd made her final payment and became the owner of the laptop, an employee of Aspen Way came to her home to repossess her computer under a mistaken belief that she had defaulted on a payment.[2] During their conversation, the employee showed her a picture of her husband, Brian Byrd, sitting in front of her laptop only hours before.[3]

Aaron's Incorporated, through its franchisee Aspen Way, had been remotely accessing Mrs. Byrd's laptop without her knowledge or consent by utilizing a spy software, DesignerWare's PC Rental Agent, installed on the machine.[4] Although the software was designed as a mechanism to track a rental laptop if it was lost or needed to be recovered, Aaron's franchisees were using the software for much more than that. The "Detective Mode" on the software allowed Aaron's employees to receive e-mails containing keystrokes, screenshots, and webcam pictures from a leased computer while it was connected to the Internet.[5] Although this type of technology has existed for at least five years, the average consumer remains oblivious to the dangers that the Internet presents to personal privacy.[6] Information such as bank statements, addresses, Social Security numbers, and phone numbers can be intercepted and stored on the servers of a company using this type of spyware.[7] Remote access to webcams without detection is a shocking thing; consumers are likely unaware of this danger to their privacy and are unprepared. If you imagine the type of actions that

---

1 *See* Byrd v. Aaron's, Inc., C.A. No. 11-101, 2011 WL 2672009, at *4 (W.D. Pa. June 16, 2011), *report and recommendation adopted sub nom*, Byrd v. Aaron's Inc., C.A. No. 11-101, 2011 WL 2672204 (W.D. Pa. July 8, 2011).

2 *Id.*

3 *Id.*

4 *Id.* at *4–5.

5 *See* Complaint at *2, *In re* Aaron's, Inc., No. 122-3264, 2013 WL 5835421 (F.T.C. Oct. 22, 2013).

6 *See, e.g.*, *id.* at *1 ("Since at least 2009 through January 2012, some Aaron's franchisees licensed a software product known as PC Rental Agent from DesignerWare . . . and installed it on computers rented to consumers."); Nicholas W. Allard, *The Globalization of Privacy and Security in Cyberspace: Government, Law, and Society in the Twenty-First Century Online World*, *in* UNDERSTANDING THE LEGAL ISSUES OF COMPUTER FORENSICS 53, 63 (2013) ("[T]he United States does not yet have an organized and determined public constituency that is advocating for the protection of individual privacy rights.").

7 *See Byrd*, 2011 WL 2672009, at *5.

may occur in front of a webcam, or the type of information that may be present on the screen of a computer at any given time, the possibilities of humiliation, invasion, and embarrassment are endless.

The Byrds brought suit in federal court under part of the Electronic Communications Privacy Act, the Wiretap Act, as well as the Computer Fraud and Abuse Act.[8] The Electronic Communications Privacy Act (ECPA) gave the Byrds a private cause of action and the right to sue for injunctive relief.[9] However, the court denied them injunctive relief.[10] This decision reflects the alarming lack of protection for individual rights when they are compromised by spyware that can literally see you. The Computer Fraud and Abuse Act has been used to deal with physical intrusions on computers,[11] while the ECPA prohibits certain types of access to stored communications and the interception of electronic communications.[12] However, courts have struggled to apply these laws as technology has advanced.[13]

Even though the unknown usage of a personal webcam to take pictures of individuals in their home or workplace is a grievous violation of personal privacy, it has not been satisfactorily addressed in court or by legislation but rather merely noted with outrage in the news.[14] In this Note I discuss the dangers that spyware and the usage of information through the Internet present to personal privacy, and I review the ECPA, its application and interpretation by the courts, and its shortcomings. Part I gives the statutory background of the ECPA and the judicial history of the interception of electronic communica-

---

8 *Id.* at *1.

9 *See* 18 U.S.C. §§ 2511(4)–(5), 2520(a)–(b) (2012).

10 Byrd v. Aaron's Inc., C.A. No. 11-101, 2011 WL 2672204, at *1 (W.D. Pa. July 8, 2011).

11 *See* 18 U.S.C. § 1030(a) (2012).

12 *See id.* §§ 2510–22, 2701–12.

13 *See, e.g.*, United States v. Councilman (Councilman II), 373 F.3d 197, 203–04 (1st Cir. 2004), *vacated*, 418 F.3d 67 (1st Cir. 2005) ("The Wiretap Act's purpose was, and continues to be, to protect the privacy of communications. . . . [M]uch of the protection may have been eviscerated by the realities of modern technology. We observe, as most courts have, that the language may be out of step with the technological realities of computer crimes."), *reh'g granted, opinion withdrawn*, 385 F.3d 793 (1st Cir. 2004) (en banc), *and on reh'g*, 418 F.3d 67 (1st Cir. 2005) (en banc); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) ("We observe that until Congress brings the laws in line with modern technology, protection of the Internet . . . will remain a confusing and uncertain area of the law.").

14 *See, e.g.*, Kealan Oliver, *Suit: Lower Merion School District Allegedly Spied on Students Through Webcams*, CBS NEWS (Feb. 19, 2010, 12:20 PM), http://www.cbsnews.com/news/suit-lower-merion-school-district-allegedly-spied-on-students-through-webcams ("A federal lawsuit filed by . . . a student at Harriton High and his parents, claims the school remotely spied on their son at home through a webcam on a laptop the school had given him."); Matt Peckham, *Rent-to-Own Outfit Allegedly Spied on PC Customers with Webcams*, TIME (May 3, 2011), http://techland.time.com/2011/05/03/rent-to-own-outfit-allegedly-spied-on-pc-customers-with-webcam ("Aaron's Inc. may have . . . stepped all over its customers' privacy rights." (emphasis omitted)).

tions under the ECPA. Part II analyzes the dangers that the Internet has brought to individual privacy, recent case law dealing with advanced spyware technology, and the "WebcamGate" scandal. Part III emphasizes that Internet spyware and the usage of information over the Internet is a serious threat to privacy, critically examines some proposed amendments to the ECPA, and calls for legislative involvement in protecting individual Internet privacy rights. Ultimately, I conclude that state law protection is not sufficient and that federal law should protect privacy and the Internet as a form of interstate commerce. In order to do so, the ECPA should be amended to include protection of any information accessible on a computer while it is connected to the Internet as "electronic communications."

I
BACKGROUND

A. Statutory Background

1. *The ECPA*

Congress enacted the Electronic Communications Privacy Act in order to update existing federal surveillance law, but most of its provisions were enacted in 1986, before the existence of the public Internet and its many avenues of communication: online chatting, banking, video conferencing, and social media.[15] However, it was enacted to deal with e-mail and the unauthorized interception of electronic communications.[16] The ECPA is broken into three titles, which are commonly referred to as the Wiretap Act,[17] the Stored Communications Act,[18] and the Pen Registry Act.[19] The Pen Registry Act prohibits any devices that record contact information such as phone numbers or e-mail addresses[20] and is not pertinent to privacy invasions from keylogger spyware that can also capture screenshots and webcam pictures. The Wiretap Act and the Stored Communications Act (SCA) have traditionally been used to monitor the unauthorized access of electronic communications.[21]

---

15 *See* Charles H. Kennedy, *An ECPA for the 21st Century: The Present Reform Efforts and Beyond*, 20 COMMLAW CONSPECTUS 129, 129 (2011); Katherine A. Oyama, Note, *E-Mail Privacy After* United States v. Councilman*: Legislative Options for Amending ECPA*, 21 BERKELEY TECH. L.J. 499, 499 (2006).

16 *See* S. REP. NO. 99-541, at 2–3, 8, 10–11 (1986).

17 18 U.S.C. §§ 2510–22 (2012); Paul Koob, Comment, *Not Enough Fingers in the Dam: A Call for Federal Regulation of Keyloggers*, 28 TEMP. J. SCI. TECH. & ENVTL. L. 125, 129 (2009).

18 18 U.S.C. §§ 2701–11 (2012).

19 *Id.* §§ 3121–27.

20 *See* Koob, *supra* note 17, at 129.

21 *See, e.g.*, Oyama, *supra* note 15, at 499–500 ("[The] ECPA provides the statutory framework governing the interception of electronic communications under the Wiretap Act and access to stored electronic communications under the SCA." (footnote omitted)).

The Wiretap Act provides that an individual shall be punished or subject to suit if he or she "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[22] There are four exceptions for the government or Internet service providers that do not apply when an unauthorized third party makes an intrusion through direct physical intervention or spyware.[23] The Wiretap Act defines an electronic communication as the "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."[24] Originally, there was a difference in the Act's language between the definition of a "wire communication" and an "electronic communication" that created ambiguity as to how stored wire and electronic communications fit into the statutory scheme.[25] Congress amended the definition of "wire communication" in order to clarify that all stored communications were regulated by the SCA, not the Wiretap Act.[26]

The Wiretap Act defines "intercept" 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."[27] There is no indication of when the communication can be intercepted, but there is a clear difference between a communication while it is being intercepted and a communication in storage,[28] which will be discussed in this Part. The Wiretap Act allows aggrieved individuals to sue for an injunction or to bring a civil action in court.[29]

The SCA broadly prohibits unauthorized access to stored communications.[30] It is illegal if an individual "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

---

22 18 U.S.C. § 2511(1)(a) (2012).

23 *See id.* § 2510(12); United States v. Councilman (Councilman III), 418 F.3d 67, 72 (1st Cir. 2005) (discussing the government's argument defining electronic communication and noting that there are "four specific exceptions not relevant here").

24 18 U.S.C. § 2510(12) (2012).

25 *See* Samantha L. Martin, Note, *Interpreting the Wiretap Act: Applying Ordinary Rules of "Transit" to the Internet Context*, 28 CARDOZO L. REV. 441, 451–52 (2006).

26 *See* USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001); *see also* Oyama, *supra* note 15, at 504 ("In 2001, Congress passed the USA PATRIOT Act and amended ECPA's definition of 'wire communication' by moving the protection of stored voice communications . . . from the Wiretap Act to the SCA.").

27 18 U.S.C. § 2510(4) (2012).

28 *See* Martin, *supra* note 25, at 443 (discussing the difference between communications "in transit" and "in storage").

29 *See* 18 U.S.C. § 2520(a)–(b) (2014).

30 *See id.* § 2701.

access to a wire or electronic communication while it is in electronic storage in such system."[31] Programmers developed spyware devices, generally classified as "keyloggers," that are able to access and store information on a computer; this type of access was not prohibited by the Wiretap Act because it did not fall within the SCA's specific provisions on access.[32] Additionally, the SCA's exceptions are more concerning than the ones detailed in the Wiretap Act because they offer less protection to stored communications.[33] There is an exception for conduct authorized "by the person or entity providing a wire or electronic communications service,"[34] which has enabled many Internet providers to legally access personal information. Many Internet service providers of e-mail include a notification that consumers' information may be used while it is stored with them.[35] It is subsequently more difficult for consumers to protect their privacy rights under the SCA.

2. *The Computer Fraud and Abuse Act*

The Computer Fraud and Abuse Act (CFAA) will not be my focus, but it is important to briefly recognize its uses in protecting individual privacy rights. Although the CFAA does prohibit certain individual actions, it requires a plaintiff to show a loss "aggregating at least $5,000 in value."[36] This makes it incredibly difficult for plaintiffs to receive damages for intrusions that may not have caused monetary injury. However, an individual who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains" protected information can be subject to criminal action and civil suit.[37] Keylogger software can fall under this statute if it is ruled as an "unauthorized access."[38]

---

31 *See id.* § 2701(a)(1)–(2).

32 *See*, Koob, *supra* note 17, at 140–42 ("[A]n individual using a keylogging device cannot be held responsible for the act of installing and capturing key strokes under the FWA [Wiretap Act], as there is no interception of 'electronic communications' under the statute.").

33 *See* Oyama, *supra* note 15, at 506–08 ("Overall, the SCA is considerably less stringent than the Wiretap Act.").

34 18 U.S.C. § 2701(c)(1) (2012).

35 *See, e.g.*, Derek S. Witte, *Bleeding Data in a Pool of Sharks: The Anathema of Privacy in a World of Digital Sharing and Electronic Discovery*, 64 S.C. L. REV. 717, 727 (2013) (giving examples of Facebook and Google privacy policies indicating that they may use certain consumer information).

36 18 U.S.C. § 1030(c)(4)(A)(i)(I) (2012).

37 *Id.* § 1030(a)(2).

38 *See* United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991); *see also* Koob, *supra* note 17, at 130–35 (elaborating applications of the CFAA that are relevant to "access").

B. Judicial Interpretation of the Interception of Communications Under the ECPA

1. *The Contemporaneous Requirement for "Intercept" in the ECPA*

As discussed previously, the Wiretap Act and the SCA exist to address separate privacy issues, and communications must be "intercepted" under the Wiretap Act in order for the statute to be triggered.[39] In determining whether the Wiretap Act should apply to an action, courts will look at either the definition of "intercept" or the definition of "electronic communication" in order to determine whether or not the communication was intercepted.[40] The definition of "intercept" under the ECPA may suggest the capture of communications or the access of communications in storage.

Several circuits have explicitly addressed issues concerning the Wiretap Act and the definition of "intercept."[41] In 1994, the Fifth Circuit faced the divide between the Wiretap Act and the SCA.[42] The Secret Service seized a computer belonging to Steve Jackson Games, and then government personnel read e-mails that were stored on the hard drive.[43] The court determined that Congress had not intended electronic communications in storage to be subject to interception under the definition in the ECPA.[44] This holding appeals to common sense, which dictates that there has to be a difference between intercepted communications and stored communications. By placing a real-time requirement on interception, the court stabilized the difference between the two types of data. However, it also caused further problems because of the amount of time that e-mail can take before it arrives in its recipient's inbox. An e-mail can be temporarily stored

---

39 *See supra* Part I.A.1.

40 *See, e.g.*, Koob, *supra* note 17, at 137 ("[T]he issue lies more in the definition of 'electronic communication' than 'intercept.'); Martin, *supra* note 25, at 454–55 ("Although courts have used . . . two different analyses, they have essentially been answering the same question—whether the communication was in the process of transmission at the time of its acquisition.").

41 *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003) ("Every circuit court to have considered the matter has held that an 'intercept' under the ECPA must occur contemporaneously with transmission."); United States v. Steiger, 318 F.3d 1039, 1048–49 (11th Cir. 2003) ("[W]e hold that a contemporaneous interception—*i.e.*, an acquisition during 'flight'—is required to implicate the Wiretap Act with respect to electronic communications."); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002) ("[T]o be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage."); Steve Jackson Games, Inc., v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994) ("[A]n intercept 'require[s] participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication . . . .'" (quoting United States v. Turk, 526 F.2d 654, 658 (5th Cir. 1976))).

42 *Steve Jackson Games*, 36 F.3d at 458.

43 *Id.* at 459.

44 *Id.* at 461–62.

but still be in transit to its destination.[45] This prompted evaluation of the second prong of the Wiretap Act, the definition of "electronic communication."

2. United States v. Councilman *and "Electronic Communication"*

While *United States v. Councilman* deals directly with e-mail privacy, the court's evaluation of the definition of "electronic communication" deserves discussion here.[46] The court in *Councilman* was forced to determine whether access of e-mails while they were in temporary storage was a violation of the Wiretap Act or the SCA.[47] The court ultimately concluded that an e-mail, during its transfer through the Internet, is stored repeatedly.[48] The court detailed the process of transmission and stated that Congress did not intend to remove electronic communications from the scope of the Wiretap Act when they are being temporarily stored.[49] Therefore, the definition of "electronic communication" must include "transient" storage that is "intrinsic to the communication process."[50]

This determination that access of transient storage is punishable under the Wiretap Act brought to light the shortcomings of the provisions of the ECPA. Because of emerging technologies, some of the definitions do not adequately describe the reality of information transfer over the Internet. This decision significantly altered conceptions on the Wiretap Act and led to calls for the amendment of definitions in the ECPA.[51] It also led to an examination of keylogger software that did not transmit immediately from a computer or did not transmit information while the computer was connected to the Internet. Does the gathering of this type of information violate the Wiretap Act?

3. United States v. Ropp *and "Electronic Communication"*

The definition of "electronic communication" was examined in relation to a type of keylogger spyware in *United States v. Ropp*.[52] The keylogger used in this case recorded and stored keystrokes so that an individual in possession of the device could access them later, thereby

---

45 *See* Martin, *supra* note 25, at 443.

46 United States v. Councilman (Councilman II), 373 F.3d 197, 199–200 (1st Cir. 2004), *reh'g en banc granted, opinion withdrawn*, 385 F.3d 793 (1st Cir. 2004), *and on reh'g en banc*, 418 F.3d 67 (1st Cir. 2005).

47 *Id.* at 203.

48 *See* United States v. Councilman (Councilman III), 418 F.3d 67, 69–79 (1st Cir. 2005).

49 *See id.*

50 *Id.* at 85.

51 *See, e.g.*, Oyama, *supra* note 15, at 518 (arguing for a clearer definition of "intercept" under the ECPA).

52 *See* United States v. Ropp, 347 F. Supp. 2d 831, 831–32 (C.D. Cal. 2004).

"eavesdropping" on an individual through a computer.[53] The device only operated within the confines of the computer, just like the interception that occurred in *Councilman*.[54] However, *Councilman* involved e-mail transmitted between computers,[55] whereas the intercepted keystrokes in *Ropp* were transmitted within the computer.[56] The system of transmission does not affect interstate commerce, and the keystrokes that were intercepted were in preparation for an electronic communication, not a communication itself.[57]

This definition of electronic communication ensured that a transmission is within a network, not simply within a system. Simple typing on a computer is not a communication because the action of keystrokes does not create a communication unless the keystrokes are going beyond the computer. Keyloggers such as these may be attacked by the SCA or the CFAA, but courts have held that they are not illegal under the Wiretap Act, leaving a loophole in the ECPA that compromises personal privacy.[58]

II
ANALYSIS

A. Increasing Risks to Personal Privacy

1. *The Right to Information Privacy*

The right to privacy, and especially the right to privacy of information, is sometimes assumed in today's world because of the Supreme Court's decision that everyone has a right to privacy.[59] The specific right to information privacy can be defined as the right an individual has to control how his or her personal information is "acquired, disclosed, and used."[60] The Clinton Administration had an Information Infrastructure Task Force, which defined personal information as "information identifiable to the individual."[61] The government also stated that "an individual's reasonable expectation of

---

53 *See id.*

54 *See id.* at 837.

55 *Councilman III*, 418 F.3d at 69–72.

56 *See Ropp*, 347 F. Supp. 2d at 837.

57 *See id.* at 837–38.

58 *See, e.g.*, *id.* (acknowledging the loophole created in holding that a keylogger did not violate the Wiretap Act).

59 *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

60 Henry M. Cooper, *The Electronic Communications Privacy Act: Does the Answer to the Internet Information Privacy Problem Lie in a Fifteen-Year-Old Federal Statute? A Detailed Analysis*, 20 J. MARSHALL J. COMPUTER & INFO. L. 1, 3 (2001) (quoting Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1205 (1998)).

61 *See id.*

privacy regarding access to and use of his or her personal information should be assured."[62]

However, there is concern as to retaining the right to information privacy. In a recent article, Derek S. Witte asserts that we are "bleeding" data and that it is "necessary to insist on a right to protect oneself from the discovery of private information."[63] He claims that the current federal laws do not create a comprehensive right to privacy, comparing the numerous federal privacy statutes and their application to information, the Internet, and the individuals regulated.[64] Many of the privacy laws are not aimed toward individual privacy rights but are instead focused on protecting individuals from the government and corporate privacy.[65] The most danger to personal privacy results from corporations that have license to invade on personal privacy, corporations such as Facebook or Google.[66] Now, corporations like Aaron's are capable of using software to spy on their customers.[67] This spyware is readily available and legal in today's market; what is preventing other corporations like Dell, Apple, or Hewlett-Packard from doing the same? There are multiple loopholes in the ECPA that allow for intrusions such as information gathering, as well as the use of keyloggers to obtain keystrokes, screenshots, and webcam pictures.

2. *Loopholes in the ECPA*

There are multiple loopholes in the ECPA that have been noted and criticized since the advent of the Internet and advanced spyware. The first major issue is that the definitions of "intercept" and "electronic communication" are still ambiguous, forcing courts to note that this area of the law is uncertain.[68] Samantha L. Martin argues that the real world precedent of "transit" should apply to electronic

---

62 Christine A. Varney, Fed. Trade Comm'n, Remarks at the Privacy and American Business Conference: Privacy in the Electronic Age *2 (Nov. 1, 1995), 1995 WL 643418 (F.T.C.).

63 *See* Witte, *supra* note 35, at 741.

64 *See id.* at 742–47 (detailing in chart form the different statutes, who they regulate, what type of information they protect, whether they are applicable to Facebook and Google, and any exceptions to their general rules).

65 *See* Allard, *supra* note 6, at 62 ("To date, many if not most of the so-called cyberlaw privacy bills deal with either corporate intellectual property or security, or protection of government functions, as opposed to individuals' rights and liberties. Curiously, there is not yet a powerful, vocal constituency for the protection of individual privacy in the United States.").

66 *See* Witte, *supra* note 35, at 748.

67 *See* Byrd v. Aaron's, Inc., C.A. No. 11-101, 2011 WL 2672009, at *4 (W.D. Pa. June 16, 2011*) report and recommendation adopted sub nom,* Byrd v. Aaron's Inc., C.A. No. 11-101, 2011 WL 2672204 (W.D. Pa. July 8, 2011).

68 *See, e.g.*, Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) ("[U]ntil Congress brings the laws in line with modern technology, protection of the Internet and websites such as Konop's will remain a confusing and uncertain area of the law."); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994)

communications as they did in *Councilman*.[69] She argues that the definition of "intercept" should also include any contemporaneous acquisitions while e-mails are in temporary storage.[70]

E-mail is the least protected when it is in electronic storage, after it is delivered to a recipient.[71] Upon close examination, there are several exceptions to the SCA that cause issues for both electronic communications and e-mail in storage. For instance, if a service provider of electronic communication has stored information for over 180 days, the government can require the provider to disclose the information without notice to the customer.[72] This loophole has caused some stir in the media, but has not been addressed by the legislature recently.[73] This affords lesser protection to electronic communication than private letters because the government does not need a warrant.[74]

Another pertinent issue is the exception granted to Internet service providers.[75] Internet service providers have immunity from unlawful activity such as surveying e-mail simply because they provide the service.[76] It appears as though there is an industry standard that allows Internet service providers such as MSN, Google, AOL, and AT&T to read their customer's e-mail.[77] After Katherine A. Oyama compared these policies in 2006,[78] not much has changed with Apple, Google, and Facebook policies today.[79] These providers also have

("[T]he Wiretap Act . . . is famous (if not infamous) for its lack of clarity . . . ." (citation omitted)).

69 *See* Martin, *supra* note 25, at 469–74 ("[E]lectronic communications in temporary electronic storage are 'in transit' when the storage is incidental to their transfer.").

70 *See id.*

71 *See* Cooper, *supra* note 60, at 17 ("However, ECPA Title II, in its current form, would not adequately protect an individual's personal information that was transmitted via the Internet and subsequently electronically stored in an electronic record on an e-commerce entity's server from being disclosed to the private sector.").

72 *See* 18 U.S.C. § 2703(a) (2014); *see also* Cooper, *supra* note 60, at 13 (discussing the provisions of section 2703(a)).

73 *See, e.g.*, Erin Fuchs, *No One is Talking About the Insane Law That Lets Authorities Read Any Email over 180 Days Old*, BUS. INSIDER (June 7, 2013, 3:53 PM), http://www.businessinsider.com/when-can-the-government-read-your-email-2013-6; Ryan J. Reilly, *DOJ: Electronic Communications Privacy Act's 180-Day Stored Email Rule Not 'Principled,'* HUFFINGTON POST (Mar. 19, 2013, 11:33 AM), http://www.huffingtonpost.com/ryan-j-reilly/ecpa-180-day-email-rule_b_2907846.html.

74 *See* 18 U.S.C. § 2703(a) .

75 *See id.* § 2701(c)(1).

76 *See* Oyama, *supra* note 15, at 519.

77 *See id.* at 520–22 (describing the industry standard that evolved from the privacy policies of major Internet service providers such as MSN, EarthLink, AT&T, Google, and AOL).

78 *See id.* at 520–22 nn.152–56 & 158 (quoting the privacy policies of these Internet service providers).

79 *See* Witte, *supra* note 35, at 722 ("Today, individuals commonly share data about themselves through the various services and applications of social networking and Internet productivity sites, like Facebook and Google.").

access to our whereabouts through software on our computers and on our mobile phones.[80] Courts and commentators have noted that there is a significant lack of clarification in the ECPA about the protection of geolocation data, because Congress did not anticipate this type of information or that it could be used by the government improperly.[81] Furthermore, information on what websites we visit, what we search, and our names, addresses, and e-mails can all be stored and recorded without our knowledge, sometimes even including passwords, credit card information, and Social Security numbers.[82] If all this information is accessible to the public, what prevents corporations such as data mining brokers and Internet service providers from intercepting communications directly from our computers? Isn't the use of software through the Internet to intercept keystrokes or webcam pictures similar to the gathering of personal information that happens every time we go online?

Some argue that the line should be drawn at keylogger software.[83] Paul Koob discusses the dangers of keylogger software at length, including the loophole in the ECPA that allows some keylogger software to slip through the clutches of regulation.[84] Some keylogger software intercepts keystrokes, like the software in *Ropp*, and does not transfer the information, preventing individuals from bringing suit under the Wiretap Act.[85] Koob also argues that these types of

---

80 *See id.* at 734–35. (describing how mobile service providers can track customers' locations and store that data even when customers do not grant permission).

81 *See, e.g.*, *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (remanding to protect "citizens' reasonable expectations of privacy regarding their physical movements and locations" with a warrant); Kennedy, *supra* note 15 at 147–48 ("Congress did not anticipate in 1986 that mobile telephone geolocation data would become a target of governmental surveillance, and ECPA sets no standard for governmental access to that data.").

82 *See, e.g.*, Witte, *supra* note 35, at 731 ("Even when we believe we are anonymously visiting web sites, data-mining companies, curious corporations, and the web sites themselves use tracking methods, cookies, and legal spyware to watch and store information about what we do on the Internet."); Taylor Armerding, *Data Brokers' Collection of Internet Activity Data Raises Privacy Issues*, IDG NEWS SERVICE (Nov. 7, 2013, 8:40 PM), http://news.idg.no/cw/art.cfm?id=0BA3C6AC-0925-23E5-A930D89890D4D90F ("[Big Data] companies . . . collect and sell information to marketers on everything from your marital status, whether you might be pregnant or have a newborn, have cancer, are trying to lose weight, are gay or straight, how much you make, what credit cards you use, your lines of credit, where you live, what your house cost, what kind of car you drive or if you might be looking to buy a new one, your race, occupation, political leanings, education level, have one or more children in college, have pets to what your hobbies are and more . . . .").

83 *See, e.g.*, Koob, *supra* note 17, at 128 ("Congress has struggled with the issue of keylogging devices and software.").

84 *See id.* at 137–40.

85 *See id.* at 137–38 (stating that information captured from a keyboard is not an "electronic communication" and so interception of it does not violate the Wiretap Act); Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283, 1301–05 (detailing the "'interception' problem").

keyloggers cannot be caught under the SCA because the access would not be password protected on the computer and therefore would not be an illegal access to the computer information.[86] Koob calls for either a new statute to deal with keylogger software or an amendment to the definition of "electronic communication" so that a transfer is no longer necessary while gathering information.[87] However, this would make some of the legal, useful information illegal, and could cause serious problems in social media. Moreover, most keylogger software has evolved and now works remotely through the Internet, such as the DesignerWare software used by Aaron's franchisees.[88] This type of alteration would not protect information stolen by the more accessible and invasive keylogger software of today, because even if the information is "transferred" over the Internet, the software is taking screenshots, pictures, and keystrokes that do not fit into the conventional definition of "electronic communication."[89] In order to deal with the increased danger that the Internet has presented to today's privacy rights, the current judicial interpretation of the ECPA for keylogger software must be analyzed.

B. Evolving Keylogger Technology and Case Law

1. United States v. Barrington

Keylogging technology has evolved since the decision of *United States v. Ropp*, which involved a KeyKatcher device that captured physical impulses on the cable between a keyboard and a computer.[90] While keyloggers used to be physical, they are now digital and installed as software on computers.[91] The most recent circuit case involving modern keylogging software is *United States v. Barrington*, which demonstrates the court's unwillingness to adapt the ECPA to a

---

86 *See* Koob, *supra* note 17, at 140 ("Because this information is not password protected, accessing it would not be unauthorized, and therefore lawful under the SCA.").

87 *See id.* at 150.

88 *See In re* Aaron's, Inc., File No. 122-3264, 2013 WL 5835421, at *2 (F.T.C. Oct. 22, 2013).

89 Under current case law like *Ropp*, keystrokes are not considered a transfer; however, they might be if someone is entering them into an Internet browser. *See* United States v. Ropp, 347 F. Supp. 2d 831, 837–38 (C.D. Cal. 2004) (holding that keylogging transmissions did not constitute "electronic communication[s]" because the transmissions did not involve use of "the internet or any other external network"). Screenshots and pictures from webcams are not "electronic communications" because they are taken by a direct action of the keylogger software, not as part of a transmitted signal. *See* 18 U.S.C. § 2510(12) (2014) (defining "electronic communication" as requiring a "transfer . . . by a wire, radio, electromagnetic, photoelectronic or photooptical system").

90 *See* Ropp, 347 F. Supp. 2d at 831.

91 *See* United States v. Barrington, 648 F.3d 1178, 1184 n.2 (11th Cir. 2011) (recognizing that keylogging is now "accomplished through use of a dedicated software application").

change in technology.[92] In this case, two college students who wanted to change their grades and the grades of friends that were applying to graduate school concocted a plan to access the Florida A&M University system with the usage of a keylogger.[93] The students managed to install the keylogger software onto several university computers, thereby capturing the login information and passwords of several university employees, and transmitted the information through e-mail to the students.[94] This information was used to access the grading system at the university and change the grades of certain students.[95]

The court reviewed the usage of the keylogger software and stated that in order for a violation of the Wiretap Act to occur, the interception of an electronic communication must be contemporaneous, reaffirming the conventional definition.[96] The court stated:

> Conceivably, the keylogger software at issue here could be used to contemporaneously capture information or signals being transmitted beyond the user's computer. If so, this would bring the keylogger software within the definition of a scanning receiver as 'a device or apparatus that *can* be used to intercept a wire or electronic communication in violation of [the Wiretap Act].' However, the Government points to no evidence in the record showing that the keylogger at issue here had that capacity and we have found none.[97]

This holding indicates that the court was unwilling to explore the impact of advanced technology on the interpretation of the Wiretap Act portion of the ECPA. Even though the keylogger was intercepting information being entered into the computer while it was connected to the Internet and transmitting that information through the Internet by e-mail, the court decided that this type of interception is not contemporaneous.[98] This demonstrates the lack of protection that the ECPA grants to consumer information when interpreted by the courts. However, district courts have begun to tackle this issue and have started to tentatively steer the interpretation of the ECPA in the opposite direction.[99]

---

92 *See id.* at 1202–03.

93 *Id.* at 1184.

94 *Id.*

95 *Id.*

96 *See id.* at 1202 (citing United States v. Steiger, 318 F.3d 1039, 1048–49 (11th Cir. 2003)). "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." *Id.*

97 *Id.* at 1203 (quoting 18 § U.S.C. 1029(e)(8)).

98 *See id.* at 1202–03.

99 *See, e.g.*, Luis v. Zang, No. 1:11-cv-884, 2013 WL 811816, at *6–7 (S.D. Ohio Mar. 5, 2013) (citing Klumb v. Goan, 884 F. Supp. 2d 644, 661 (E.D. Tenn. 2012)) ("[S]pyware can violate the Wiretap Act if it transmits captured or recorded information over the

2. *District Court Decisions*

Several district courts have faced complaints involving new keylogging spyware software such as SpectorPro, PC Rental Agent, and WebWatcher.[100] These keyloggers are digital spyware that challenge the conventional definition of "contemporaneous interception" and more or less work the same way, including taking screenshots, recording keystrokes, and activating the webcam of a computer.[101] In one case, *Luis v. Zang*, an individual used the software WebWatcher to spy on his wife.[102] This software allowed him to access screenshots and keystrokes from her computer, as well as other information.[103] The court examined previous cases, such as *Barrington* and *Ropp* and determined that the keylogger software used in *Ropp* was markedly different than WebWatcher because it did not transmit information away from the computer, and that the court in *Barrington* acknowledged that keylogger software could satisfy the contemporaneous interception requirement.[104] The court suggested that a rethinking of the definition of "contemporaneous" might be necessary and that the timing of the intercepted data's transmission should be irrelevant, allowing the ECPA to be applied.[105] However, this rethinking of the definition may start to blur the line between the ECPA and the Stored Commu-

---

[I]nternet . . . ."); Arrington v. Colortyme, Inc., 972 F. Supp. 2d 733, 747 (W.D. Pa. 2013) ("Because the Complaint's allegations regarding Plaintiff's private communications are sufficient to plead the occurrence of an 'intercept' under the ECPA, the federal cause of action survives, regardless of whether the screenshots, keystrokes and webcam photographs were in transmission. Furthermore, given the sophistication of the technology at issue, it is entirely possible that discovery will reveal that the screenshots, keystrokes and pictures were in some state of 'transmission' as envisaged by the statute when they were obtained by PC Rental Agent."); Shefts v. Petrakis, No. 10-cv-1104, 2012 WL 4049484, at *9 (C.D. Ill. Sept. 13, 2012) ("There are not many cases analyzing the application of the ECPA to screen-capture technology. In light of the other ECPA precedent discussed in this Order, though, the Court must find that Defendants' use of SpectorPro constituted an interception under the ECPA.").

100 *See Luis*, 2013 WL 811816, at *1 (discussing WebWatcher); *Arrington*, 972 F. Supp. 2d at 737 (discussing PC Rental Agent); *Shefts*, 2012 WL 4049484, at *3 (discussing SpectorPro).

101 *See* Byrd v. Aaron's, Inc., CA No. 11-101, 2011 WL 2672009, at *5 (W.D. Pa. June 16, 2011) *report and recommendation adopted sub nom*, Byrd v. Aaron's Inc., No. 11-101, 2011 WL 2672204 (W.D. Pa. July 8, 2011) (explaining that an employee oversaw the keystrokes, screenshots, and photographs that the PC Rental Agent software collected); *SpectorPro Product Overview*, SpectorSoft, http://www.spectorsoft.com/products/SpectorPro_Windows/index.asp (last visited Apr. 19, 2015) (listing screenshots, keystrokes, and remote viewing among its monitoring capabilities); *WebWatcher–Features*, WebWatcher, http://www.webwatcher.com/#features (last visited Apr. 19, 2015) (detailing how the software can record keystrokes and screenshots, but unclear as to whether or not the software has webcam access).

102 *Luis*, 2013 WL 811816, at *1 (S.D. Ohio Mar. 5, 2013).

103 *See id.* at *6.

104 *See id.* at *5–6.

105 *See id.* at *6–7 (citing Klumb v. Goan, 884 F. Supp. 2d 644, 661) (E.D. Tenn. 2012)).

nications Act, bringing back the problem presented in *United States v. Councilman* of what is stored and what is a transmission.[106]

Another court in the Western District of Pennsylvania dealt with the argument that the information obtained from the PC Rental Agent software was not in transmission when it was accessed.[107] The court stated that in light of the technology's sophistication, it is possible that the information was in "transmission" as defined by the statute, and that the plaintiff had a claim that should not be dismissed.[108] A third court in the Central District of Illinois took this reasoning further, ruling that the usage of a similar spyware called SpectorPro was in violation of the ECPA.[109] The court in *Shefts v. Petrakis* stated:

> Plaintiff puts on undisputed evidence that the SpectorPro software caused images of Plaintiff's computer activity, including his communications via his Yahoo! email account, to be simultaneously captured by SpectorPro. . . . [A]ny emails sent by Plaintiff on his Yahoo! account via his desktop computer would have been captured by SpectorPro *as they were transmitted* to Yahoo! via the internet. Therefore, SpectorPro contemporaneously captured Plaintiff's electronic communications within the meaning of the ECPA, and Defendants were able, if they were at the monitoring station while Plaintiff was using his Yahoo! email account, to view Plaintiff's communications as he viewed them.[110]

This clearly indicates that this court was willing to accept that modern keylogger spyware is able to intercept information from a computer contemporaneously when the information is being transferred over the Internet. However, this ruling is very narrow, as it does not address screenshots taken of Microsoft Word documents or other information entered into a computer but not directly through the Internet. It also does not address the issue of webcam pictures. While courts could eventually construe the ECPA to include information directly entered into an Internet browser as the court in *Shefts v. Petrakis* did, this still leaves any other computer activity and unwanted webcam pictures outside the statute's protection. Only one court has publicly faced the webcam issue: the court in the case of *Robbins v. Lower Merion School District*.[111]

---

106 *See supra* Part I.B.2.

107 *See* Arrington v. Colortyme, Inc., 972 F. Supp. 2d 733, 747 (W.D. Pa. 2013).

108 *See id.*

109 *See* Shefts v. Petrakis, No. 10-cv-1104, 2012 WL 4049484, at *11 (C.D. Ill. Sept. 13, 2012).

110 *Id.* at *9.

111 No. 10-665, 2010 WL 1957103, at *1 (E.D. Pa. May 14, 2010) (enjoining school district from remotely activating webcams on student laptops).

C. *Robbins v. Lower Merion School District*

1. *Court Grants Injunctions*

In February 2010, a group of students and parents sued the Lower Merion School District in a class action lawsuit, outraged by the discovery that the school district had been taking videos and photographs of students by utilizing software called Lan Rev.[112] The school district had launched an initiative that allowed every child to receive a laptop in order to have 24/7 access to resources and school related activities.[113] Parents and students did not know that the school district could remotely activate the webcams until an assistant principal at a high school informed Blake Robbins that she believed that he had engaged in improper behavior in his home, and she used a photo that was clearly from Blake's webcam as evidence.[114]

The first charge that the plaintiffs brought against the Lower Merion School District was one under the ECPA.[115] The plaintiffs brought a claim under section 2511 and section 2520 of the ECPA, claiming that the school district had illegally intercepted electronic communications.[116] The ECPA section 2511 states:

> [A]ny person who—(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any . . . electronic communication . . . [or] (d) intentionally uses, or endeavors to use, the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the interception of a[n] . . . electronic communication in violation of this subsection . . . shall be punished . . . or shall be subject to suit . . . .[117]

The ECPA section 2520 explains the relief that is available to plaintiffs who sue for a violation of the Act, which could include preliminary or declaratory relief, damages, punitive damages, and litigation costs.[118] The second charge brought by the plaintiffs was under the Computer Fraud and Abuse Act section 1030.[119] This statute forbids the unauthorized access of a computer and prohibits taking information from a protected computer, but it is challenging to pursue damages under

---

112 *See* Robbins *ex rel.* Robbins v. Lower Merion Sch. Dist., No. 10-665, 2010 WL 3421026, at *1 (E.D. Pa. Aug. 30, 2010).

113 *See* Class Action Complaint at 6, Robbins v. Lower Merion Sch. Dist., 2010 WL 581793 (E.D. Pa. Feb. 16, 2010).

114 *See id.*

115 *See id.* at 7–9 ("The software/hardware used by the School District to remotely activate the webcams complained of constitute an 'electronic . . . device' within the meaning of 18 U.S.C. § 2510(5). By using said software/hardware to secretly obtain webcam images, each Defendant 'intercepts' that communication within the meaning of § 2511.").

116 *See id.*

117 18 U.S.C. § 2511(1) (2012); *see supra* Part I.A.1.

118 *See* 18 U.S.C. § 2520 (2012); *supra* Part I.A.1.

119 *See* Class Action Complaint, *supra* note 113, at 10–11.

this statute because the relief is narrower than that of the ECPA.[120] The plaintiffs also brought claims under the Stored Communications Act, the Civil Rights Act, the Fourth Amendment, and state law.[121]

The court issued a series of preliminary injunctions against the school district's further usage of the spyware.[122] The court stated that "[e]xcept as otherwise provided in this paragraph, [the school district] is enjoined from purchasing any software, hardware, or other technology that allows for the remote activation of webcams on student laptops or the remote monitoring or recording of audio or video from student laptops."[123] However, the court did not explain its reasoning in any of its three official orders.[124] The court also did not explain its reasoning in a written opinion because the case settled well before trial.[125] Therefore, even though the court granted injunctions, it is unclear what law and charges the court depended on. Furthermore, because the case settled, the law—or lack of laws—concerning this type of invasion of privacy was not addressed, and the court was not able to present the legal community with a precedent. However, the case did spark outrage in the media and a proposed amendment.

2. *"WebcamGate"*

Although consumers appear to turn a blind eye to the usage of geolocation information, web browsing, and data mining for targeted advertising,[126] the media outrage sparked by this intrusion of privacy was anything but blind and forgiving. Local news and national media outlets reported on the story, which led to a federal investigation into wiretap laws.[127] One source indicated that the students at Harrington High School where this drama unfolded had nicknamed the situation

---

120 *See* 18 U.S.C. § 1030; *supra* Part I.A.2.

121 *See* Class Action Complaint, *supra* note 113, at 11–15.

122 *See* Robbins *ex rel.* Robbins v. Lower Merion Sch. Dist., No. 10-665, 2010 WL 3421026, at *1 (E.D. Pa. Aug. 30, 2010).

123 Robbins *ex rel.* Robbins v. Lower Merion Sch. Dist., No. 10-665, 2010 WL 1976869 (E.D. Pa. May 14, 2010).

124 *See id.* at *1–3; Robbins *ex rel.* Robbins v. Lower Merion Sch. Dist., No. 10-665, 2010 WL 3421026, at *1–8; Robbins v. Lower Merion Sch. Dist., No. 10-665, 2010 WL 1957103, at *1–2.

125 *See* Adam B, *WebcamGate Has Settled: $610,000*, DAILY KOS (Oct. 12, 2010, 7:53 AM) http://www.dailykos.com/story/2010/10/12/909702/-WebcamGate-Has-Settled-610-000.

126 *See supra* Part II.A.2.

127 *See, e.g.*, Jennifer Abel, *Webcamgate case resolved. Badly*, GUARDIAN (Oct. 16, 2010, 8:00 PM), http://www.theguardian.com/commentisfree/cifamerica/2010/oct/16/little-merion-webcamgate (criticizing the settlement of the case between the school district and the students); Larry King, Dan Hardy & John Shiffman, *Webcam Issue Is New Frontier: Cyber-spying Suit Is Unprecedented, Experts Say. A Federal Probe Is Said to Focus on Wiretap Laws.*, INQUIRER (Feb. 21, 2010), http://articles.philly.com/2010-02-21/news/25218818_1_wire-tap-school-issued-laptop-spy (discussing the lawsuit filed against the Lower Merion School District and the public's response); Vince Lattanzio, *WebcamGate Teen: "I Hope They're Not Watching Me*," NBC PHILA. (Feb. 22, 2010, 8:59 AM), http://www.nbcphiladelphia.com/

"WebcamGate," and that school officials had originally installed the software in order to track and retrieve stolen laptops.[128] Unfortunately, software that can be very useful for retrieving stolen goods can also be used for other purposes; in this case, Blake Robbins' webcam was turned on and recorded him eating a couple of Mike and Ike candies, leading school officials to somehow believe that he was involved in drugs.[129] Senator Arlen Specter held a Senate hearing investigating this matter in order to determine whether or not federal legislation was needed to protect individuals, especially minors, from webcam surveillance.[130] One group that testified at the hearing, the Electronic Frontier Foundation, reported that they strongly urged the Senator to push for new protections against video surveillance, especially because the gap in the law on video surveillance had been known to exist since at least 1984.[131] Several media outlets reported on the WebcamGate settlement, highlighting the lack of ramifications for the district even in light of changes in policy, including the fact that the administrators that were in charge of the software were able to keep their jobs.[132] Senator Specter introduced the Surreptitious Video Surveillance Act of 2010 because of the continued lack of protection against webcam spying.[133]

As courts noted in cases such as *Barrington* and *Shefts v. Petrakis,* technology has changed significantly since Congress passed the ECPA

---

news/local/WebcamGate-Teen-I-Hope-Theyre-Not-Watching-Me-84826357.html (reviewing the case against the school district and discussing the reaction of the students).

128 *See* King, Hardy & Shiffman, *supra* note 127 ("The . . . school district said the cameras were activated only on laptops that had been reported missing, lost or stolen. This school year, technicians activated the system 42 times and retrieved 18 missing or stolen laptops - before last week's controversy caused officials to disable the system till further notice.").

129 *See* Lattanzio, *supra* note 127.

130 *See* Vince Lattanzio, *Specter Holding Hearing on WebcamGate Case*, NBC PHILA. (Mar. 16, 2010, 10:00 PM), http://www.nbcphiladelphia.com/news/tech/Specter-Holding-Hearing-on-WebcamGate-Case-87955817.html.

131 *See* Kevin Bankston, *Senators Introduce Bill in Response to EFF's Call for New Protections Against Secret Video Surveillance*, ELECTRONIC FRONTIER FOUND. (Apr. 15 2010), https://www.eff.org/deeplinks/2010/04/senators-introduce-bill-response-effs-call-new ("Of course it is anomalous to have detailed statutory regulation of bugging and wiretapping but not of television surveillance, in Title III . . . and we would think it a very good thing if Congress responded to the issues discussed in this opinion by amending Title III to bring television surveillance within its scope." (quoting United States v. Torres, 751 F.2d 875, 885 (7th Cir. 1984))).

132 *See, e.g.*, Abel, supra note 127 ("So what happened to the school administrators . . . who spied on teens at home, then lied about the extent of it? Nothing. No jobs lost and no financial consequences, either . . . ."); Dan Stamm, *School District Settles WebcamGate*, NBC PHILA. (Oct. 12, 2010, 8:48 AM), http://www.nbcphiladelphia.com/news/breaking/Lower-Merion-Webcam-Settlement-104746984.html ("Earlier this summer, the U.S. Attorney's Office, the FBI and the Montgomery County District Attorney cleared the District, and its employees—current and former—of any criminal wrongdoing.").

133 *See* Surreptitious Video Surveillance Act of 2010, S. 3214, 111th Cong. (2010); Bankston, *supra* note 131.

and other communication privacy laws.[134] This proposed legislation by Senator Specter was not enacted as law, and there have been other proposed amendments and laws that concern electronic communication privacy that have also been unsuccessful.[135] As evidenced by the alarming WebcamGate scandal that demonstrates the lack of legal protection consumers have, it is clear that the ECPA and the CFAA are outdated and have left courts in a difficult position; only recently have courts begun to attempt to fit spyware into the current definition of the ECPA.[136] In order to protect consumers from spyware that is capable of obtaining any and all information from a computer, from keystrokes to pictures of the user, the legislative branch must take action. Failed legislation must be examined to determine how best to proceed against this problem, which is becoming more and more relevant in society today, as shown by the public's reaction to Edward Snowden.[137]

III
Recommendation For Greater Legislative Action

It is clear that the ECPA needs to protect a greater range of data than it already does. I propose that the definition of "electronic communication" be altered to include "all information accessible to a computer while it is connected to the Internet." While a computer is connected to the Internet, all of the information on the computer has the possibility of being accessed. From Microsoft Word documents to webcam pictures, anything a computer has access to should be considered an "electronic communication" when the Internet is involved. This would prevent keylogger spyware from obtaining any information on a computer illegally, and it would prevent a keylogger from using a webcam, because as soon as the webcam turns on, the information obtained by it becomes an electronic communication transmitted by the computer. This type of reform would allow Congress to impose regulations on actions taken by individuals obtaining information illicitly and invading the privacy of consumers. The usage of information obtained through the Internet, such as Web history, could fall underneath this act, if Congress so desired. That would cause problems for

---

134 *See supra* Part II.B.1–2.

135 *See* Surreptitious Video Surveillance Act of 2010; Internet Spyware (I-SPY) Prevention Act of 2007, H.R. 1525, 110th Cong. (2007); Securely Protect Yourself Against Cyber Trespass Act, H.R. 964, 110th Cong. (2007); E-mail Privacy Act of 2005, S. 936, 109th Cong. (2005).

136 *See supra* Part II.B.2.

137 *See Edward Snowden: Timeline*, BBC News (Aug. 20, 2013), http://www.bbc.co.uk/news/world-us-canada-23768248 (describing the timeline of events involving Edward Snowden leaking intelligence information and disclosing the existence of certain U.S. government surveillance programs).

targeted advertising and the usage of geolocation data, but those problems could easily be addressed by the courts or if Congress wishes to add exceptions that detail how information obtained through the Internet can be used.

Other solutions have been offered in the past, but as I will demonstrate, these solutions will fall short, and Congress has failed to pass legislation that is overly broad. This simple definition change would allow Congress to make a change in the current legislative landscape without drastically altering enforcement and expectations. An alternative to legislative action lies with the Federal Trade Commission, which has brought consumer suits against companies that use invasive technology in the past.[138] The Federal Trade Commission has settled such disputes, much like how litigants have chosen to settle with the defendants in cases that involved invasive technology such as PC Rental Agent.[139] Settlements are less expensive and less time consuming, so it stands to reason that many plaintiffs will choose this route, leaving the judicial and legislative landscape relatively untouched for future unhappy explorers. Instead of relying on government enforcement through the FTC, Congress must act through legislation by changing the definition of "electronic communication." Prior proposed legislation has not been successful thus far.

A. Proposed Legislation

It is clear that Congress is not blind to the fact that there is a need for legislation involving electronic communication privacy, especially legislation that addresses the problems that occur with the use of the Internet. Over the last decade, multiple bills have been submitted and rejected, a few of which include the Surreptitious Video Surveillance Act of 2010, the E-mail Privacy Act of 2005, the I-Spy Act, and the Spy Act.[140] The Surreptitious Video Surveillance Act of 2010, introduced by Senator Arlen Specter after the WebcamGate scandal, moves to make unauthorized video surveillance a criminal offense when the individual is in a place that is not easily observable and has a

---

138 *See* Press Release, Fed. Trade Comm'n, FTC Halts Computer Spying (Sept. 25, 2012), http://www.ftc.gov/news-events/press-releases/2012/09/ftc-halts-computer-spying; *see also* Complaint at *5, *In re* Aaron's, Inc., File No. 122-3264, 2013 WL 5835421 (F.T.C. Oct. 22, 2013) (stating that Aaron's practices constituted unfair acts in violation of section 5 of the FTC Act, 15 U.S.C § 45(a)).

139 *See* Press Release, Fed. Trade Comm'n, Aaron's Rent-To-Own Chain Settles FTC Charges That it Enabled Computer Spying by Franchisees (Oct. 22, 2013), http://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chain-settles-ftc-charges-it-enabled-computer.

140 Surreptitious Video Surveillance Act of 2010, S. 3214, 111th Cong. (2010); Internet Spyware (I-SPY) Prevention Act of 2007, H.R. 1525, 110th Cong. (2007); Securely Protect Yourself Against Cyber Trespass Act, H.R. 964, 110th Cong. (2007); E-mail Privacy Act of 2005, S. 936, 109th Cong. (2005).

reasonable expectation of privacy.[141] Although there is no public reason for the denial of this bill, this type of criminalization would be difficult to enforce and may cause certain activities that should be legal to become illegal, such as video surveillance for purposes of theft protection. This bill did not address the ECPA or the CFAA, which were the statutes utilized by the plaintiffs in the WebcamGate scandal.[142] This type of legislation appears to be too broad and does not address the issue of spyware that can access any information on a computer, whether or not that information is being transmitted through the Internet.

Another option presented was the E-Mail Privacy Act of 2005.[143] This act moved to deal with the problems presented by *United States v. Councilman* and the nature of e-mail transmission.[144] Because the Wiretap Act has more stringent requirements than the Stored Communications Act, this amendment proposed to include the interception of e-mails in storage as an interception of an electronic communication.[145] The proposed change to the Wiretap Act was as follows:

> Section 2510(4) of title 18, United States Code, is amended by striking "through the use of any electronic, mechanical, or other device." and inserting "contemporaneous with transit, or on an ongoing basis during transit, through the use of any electronic, mechanical, or other device or process, notwithstanding that the communication may simultaneously be in electronic storage[.]"[146]

While this definition would remove the problem presented by stored e-mail, and perhaps could allow protection for stored information on a computer that is not necessarily transmitted over the Internet, this change would blur the line between the Wiretap Act and the SCA. The legislature specifically divided electronic communications and their storage into two separate regulations,[147] so this monumental

---

141 *See* S. 3214 ("To prohibit any person from engaging in certain video surveillance except under the same conditions authorized under chapter 119 of title 18, United States Code, or as authorized by the Foreign Intelligence Surveillance Act of 1978.").

142 *See* Class Action Complaint at 9–10, Robbins v. Lower Merion Sch. Dist., 2010 WL 581793 (E.D. Pa. Feb. 16, 2010).

143 *See* S. 936.

144 *See supra* Part I.B.2.

145 *See* Martin, *supra* note 25, at 476 ("If law enforcement is required to meet the Wiretap Act's rigorous requirements for obtaining electronic communications in transient electronic storage, law enforcement may end up using methods such as 'sniffer devices' less often (since they may be unable to meet the Wiretap Act requirements) and therefore will impose on individual liberties less often.").

146 S. 936.

147 *See* 18 U.S.C. § 2511(1)(a) (2012) (regulating the interception of "electronic communication"); 18 U.S.C. § 2701 (2012) (regulating the unauthorized access of a "facility through which an electronic communication service is provided" and the obtaining or altering of a communication while it is in storage).

change would have to be carefully examined. Furthermore, this change in the definition will not solve the identified problems (webcam surveillance, information stored on a computer obtained through keystrokes or screenshots, improper usage of data retrieved from the Internet) but will simply reorganize the law currently in place. Even if stored information is included in an electronic communication, webcam surveillance may not be considered an interception of an electronic communication and information that is not stored through the Internet may fall outside this definition. While this amendment would offer greater protection for information electronically transferred through the Internet, it does not address all of the problems the Internet presents to privacy.

It is also important to note the existence of the I-Spy and the Spy Act, neither of which passed in the Senate.[148] The I-Spy Act probably did not pass because it was an amendment to the CFAA that did not have a private right of action.[149] The I-Spy Act also did not address physical keylogger issues, which the CFAA is meant to address.[150] The Spy Act proposed an entirely new act that would enforce the "prohibition of unfair or deceptive acts or practices relating to spyware."[151] While this act did provide sufficient redress for private plaintiffs,[152] the law's scope was too narrow because it only prohibited keyloggers from obtaining personally identifiable information.[153] Paul Koob, primarily concerned with physical keyloggers, rejected the use of either of these statutes because they did not protect adequately against physical keyloggers and they were too narrow in their prohibitions.[154] Accordingly, Koob proposes to amend the ECPA's definition of electronic communication so that it no longer requires a "transfer," in order to protect against keyloggers in general.[155] I disagree with him on two points: First, altering the definition of "electronic communication" so that it does not require a transfer renders the regulation impractical because it would require the government to

148 *See* Internet Spyware (I-SPY) Prevention Act of 2007, H.R. 1525, 110th Cong. (2007); Securely Protect Yourself Against Cyber Trespass Act, H.R. 964, 110th Cong. (2007).

149 *See* Koob, *supra* note 17, at 147 ("First, the bill provides no private right of action. This absence is a huge blow to preventing the use of keylogging devices, as prosecutorial discretion may hamper the enforcement of any changes to the current federal legislation.").

150 *See id.*

151 *See* H.R. 964 § 2.

152 *See id.* § 4(b)(1) ("[T]he Commission may, in its discretion, seek a civil penalty for such pattern or practice of violations in an amount, as determined by the Commission, of not more than—(A) $3,000,000 for each violation of section 2; and (B) $1,000,000 for each violation of section 3.").

153 *See* Koob, *supra* note 17, at 148.

154 *See id.* at 147–48.

155 *See id.* at 150.

regulate inaction, instead of action that directly affects interstate commerce. Second, physical keyloggers should be regulated by the CFAA, not the ECPA, because they access a computer, not a communication.

B. The Dangers of Internet-Based Spyware and the Usage of Information Through the Internet

1. *Koob's Solution*

Koob's idea of focusing on a small change to the ECPA is sound. It is very difficult to pass new acts, as shown by the failure of the Spy Act,[156] especially when the act may deal with technology that many consumers may not understand. New sweeping legislation may introduce new loopholes and create new problems, whereas amending old laws to bridge the already existing gaps is a more practical exercise. Courts have focused on what the definitions of "intercept" and "contemporaneous" mean in today's age.[157] Instead, Koob focuses on the definition of electronic communication.[158] However, Koob suggests that the "interception problem," the issue of how individuals obtain the information, be removed from the definition of electronic communication.[159] If an electronic communication is not intercepted, how is it received? Even if the electronic communication is merely "obtained," the same problem presents itself: webcam pictures are not protected, screenshot information is not protected, and information gathered through the Internet is not protected. The main problem with the statute is not the manner in which the information is obtained; courts are becoming more willing to accept that keyloggers "intercept" electronic communications.[160] The problem is with the type of information that is not protected.

2. *The Internet Presents Far More of a Danger to Privacy than Physical Keyloggers*

The ECPA protects information obtained by physical keyloggers but leaves the data acquired by software keyloggers unprotected. To reiterate, a physical keylogger, like the KeyKatcher used in *United*

---

156 *See supra* note 140 and accompanying text.

157 *See, e.g.*, Klumb v. Goan, 884 F. Supp. 2d 644, 661 (E.D. Tenn. 2012) ("The point is that a program has been installed on the computer which will cause emails sent at some time in the future through the internet to be rerouted automatically through the internet to a third party address when the intended recipient opens the email for the first time."); Shefts v. Petrakis, No. 10-cv-1104, 2012 WL 4049484, at *9 (C.D. Ill. Sept. 13, 2012) ("Therefore, SpectorPro contemporaneously captured Plaintiff's electronic communications within the meaning of the ECPA, and Defendants were able, if they were at the monitoring station while Plaintiff was using his Yahoo! email account, to view Plaintiff's communications as he viewed them.").

158 *See* Koob, *supra* note 17, at 147–50.

159 *See id.* at 150.

160 *See supra* Part II.B.2.

States v. Ropp, is attached to a computer and captures electrical impulses, thereby recording keystrokes from a computer.[161] While it is unclear whether or not courts will see this as an interception of an electronic communication, this type of unauthorized physical access could be protected by the CFAA.[162] Regardless, this invasion of privacy is far less serious than the invasion of privacy presented by keylogger software used through the Internet. As discussed, keylogger software such as SpectorPro and PC Rental Agent can obtain pictures of a user through the webcam of the computer, record Internet history, locate the laptop or device in question, take screenshots of the computer, and record all keystrokes.[163] Furthermore, companies can track Web preferences in order to provide targeted advertising, as well as obtain the location of individuals from their cell phones.[164] Most of the time, the consequences of our actions are innocuous, so you barely notice them. When you browse a website, there is a targeted ad for the shoes you were looking at yesterday. On Facebook, you see an ad for horseback riding lessons, and you remember that you added horses to your interests last week. You allow your movie application on your phone to access your location so that you can determine which showing you want to see at the local movie theater. Some of this information is used in ways you may not know about, and some of it is used in ways that are very helpful for consumers. Regulation is needed, however, to prevent companies from overusing the information that is gained through the Internet. The tools that they use may be simplified versions of the spyware that can access your entire computer. It may be possible for the information that companies obtain through the Internet to be regulated by the ECPA, as well.

C. A Call for Greater Legislative Involvement

It is clear based on this analysis of the dangers of remotely accessible spyware and on the prior proposals to the current state of the ECPA that something less drastic and more encompassing must be done in order to protect consumers. This is the time for Congress to act, because of the recent public outrage that occurred when Edward Snowden revealed the amount of information that the government was able to obtain through the Internet from cell providers.[165] Congress is already facing pressure to restrict the government and cor-

161 *See* United States v. Ropp, 347 F. Supp. 2d 831, 831–32 (C.D. Cal. 2004).

162 *See* United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991).

163 *See supra* Part II.B.2.

164 *See* Witte, *supra* note 35, at 733–35 ("The software and service providers on our phones purportedly ask our permission to use our geolocation information for advertising purposes.").

165 *See Edward Snowden: Timeline*, *supra* note 137.

porate use of cell phone data.[166] In light of the Edward Snowden fiasco, over two dozen privacy laws have passed across the country last year.[167] These states felt the pressure of public concern over the use and collection of personal data and moved to protect their citizens.[168] This is a clear indicator that it is time for the federal government to update its privacy laws because widespread, national protection is the best way to uniformly regulate data that can be accessed through the Internet. Congress must act to protect any information contained on a computer that is accessible through the Internet to prevent any further invasions of privacy like those the Byrds and the children in the Lower Merion School District experienced.

CONCLUSION

The history of the ECPA has long been dotted with confusion. Courts and commentators alike have been baffled by the statutory construction, even after clarifying amendments and developed case law. The ECPA continues to be a confusing and inadequate protection for individual privacy. There are many loopholes in the law that courts have attempted to address. While e-mails have received more protection from the courts, there are still problems related to e-mails in storage, information stored on computers, remote activation of webcams, and information gathering by Internet service providers.

The ECPA needs amending. I propose that Congress amend the definition of "electronic communication" to include "all information accessible to a computer while it is connected to the Internet." This definition accurately describes the breadth of private, yet accessible, data that deserves the same level of protection currently afforded e-mails. This amendment will prevent corporations from spying on individuals through private webcams and gathering screenshots, while maintaining the traditional case law that is based on the definition of contemporaneous intercept with electronic communication. This amendment will change the statute the least and have the least impact on current court precedent, while enormously stretching protection for the average consumer. The time for Congress to act is now, when the public is just beginning to realize that nothing, from a Web browser to a Word document, is truly private. I just covered my webcam. Will you?

---

166 *See* Mark Jaycox, *Congress Will Battle Over Internet Privacy in 2013*, ELECTRONIC FRONTIER FOUND. (Jan. 31, 2013), https://www.eff.org/deeplinks/2013/01/congress-will-battle-over-internet-privacy-2013.

167 *See* Somini Sengupta, *No U.S. Action, So States Move on Privacy Law*, N.Y. TIMES (Oct. 30, 2013), http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html.

168 *See id.*