UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 13
Issue 2 *Spring 2012*

Article 6

3-1-2012

Carrier IQ, Pre-Transit Keystroke Logging, and the Federal Wiretap Act

Andrew D. Salek-Raham

Follow this and additional works at: http://scholarship.law.unc.edu/ncjolt

 Part of the Law Commons

Recommended Citation

Andrew D. Salek-Raham, *Carrier IQ, Pre-Transit Keystroke Logging, and the Federal Wiretap Act*, 13 N.C. J.L. & TECH. 417 (2012).
Available at: http://scholarship.law.unc.edu/ncjolt/vol13/iss2/6

This Article is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in North Carolina Journal of Law & Technology by an authorized administrator of Carolina Law Scholarship Repository. For more information, please contact law_repository@unc.edu.

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 13, ISSUE 2: SPRING 2012

CARRIER IQ, PRE-TRANSIT KEYSTROKE LOGGING, AND THE FEDERAL WIRETAP ACT

Andrew D. Salek-Raham[*]

Mobile analytics software companies must walk a fine line between providing useful data to their customers—handset manufacturers and wireless network operators—and protecting the privacy rights of consumers whose data they collect. In late 2011, a relatively unknown Connecticut-based systems administrator named Trevor Eckhart revealed that mobile analytics software developer, Carrier IQ, may have crossed this line by surreptitiously collecting outgoing cell phone numbers, SMS message text, and web addresses on user handsets. Although recent judicial decisions have narrowly interpreted the Federal Wiretap Act to exclude pre-transit keystroke logging, courts hearing the upcoming Carrier IQ class action suits should abandon these narrow interpretations in favor of a broader interpretation consistent with the Act's original purposes.

I. INTRODUCTION

In late October 2011, the market research company, International Data Corporation ("IDC")[1] praised Carrier IQ ("CIQ"),[2] a mobile analytics software developer, for being a

[*] J.D. Candidate, University of North Carolina School of Law, Class of 2013. I would like to thank the University of North Carolina Journal of Law and Technology editors and staff for their invaluable assistance throughout the writing process. I would also like to thank Professor Anne Klinefelter for her professional guidance.

[1] International Data Corporation ("IDC") is a subsidiary of International Data Group and, among other services, conducts research on information technology, telecommunications, and consumer technology companies to help investors "make fact-based decisions on technology purchases and business strategy." *About IDC*, INT'L DATA CORP., http://www.idc.com/about/about.jsp?t=1329585496880 (last visited Feb. 23, 2012).

[2] Carrier IQ is a mobile analytics software development company that specializes in collecting, storing, and analyzing handset user data on behalf of

"leading provider of Mobile Intelligence solutions" to over 141 million handset devices and named the California-based firm a 2011 "[c]ompany to [w]atch."[3] Several weeks later, a relatively unknown Connecticut-based systems administrator named Trevor Eckhart[4] posted a YouTube video[5] that simultaneously revealed both the "creepy"[6] inner workings of the cell-phone software and the irony of IDC's description, accusing CIQ of surreptitiously collecting a host of private user data, such as sent text message contents, visited web addresses, and dialed phone numbers.[7] In the

---

handset manufacturers and wireless service providers, who then use that data to improve network and product performance. *Network Operators*, CARRIER IQ, http://www.carrieriq.com/network-operators/ (last visited Mar. 21, 2012). Founded in 2005, the company's software has already been installed on over 141 million handsets. Matthew J. Schwartz, *Carrier IQ v. Wiretap Laws*, INFO. WK., http://www.informationweek.com/news/security/privacy/ 232200565 (last visited Mar. 21, 2012). Prior to accusations of surreptitious surveillance, the company was recognized not only by IDC as a company to watch, but by other groups as well. *About Carrier IQ*, CARRIER IQ, http://www.carrieriq.com/about-us (last visited Mar. 21, 2012). The *Wall Street Journal*, for example, ranked Carrier IQ ninth on its Next Big Thing 2011 List of the Top 50 Venture-Funded Companies. *Id.*

[3] Press Release, Carrier IQ, Carrier IQ Named as an Innovative Business Analytics Company Under $100M to Watch by Leading Analyst Firm (Oct. 27, 2011), *available at* http://www.carrieriq.com/documents/27-october-2011-carrier-iq-named-innovative-business-analytics-company-under-100m-to-watch-by-leading-analyst-firm/6592/.

[4] Prior to accusing Carrier IQ of suspicious data collections, Trevor Eckhart worked as a systems administrator for Intergis LLC, a sales associate at Staples, and an independent IT consultant. *Trevor Eckhart's Homepage*, TREVOR ECKHART.COM, http://trevoreckhart.com/index.html (last visited Feb. 23, 2012). A self-proclaimed skilled programmer, he is also an "Eagle Scout & rock/roller." *Id.*

[5] *Carrier IQ Part #2*, YOUTUBE (NOV. 28, 2011), http://www.youtube.com/watch?v=T17X QI_AYNo&feature=player_embedded.

[6] Gerry Smith, *Carrier IQ: Researcher Trevor Eckhart Outs Creepy, Hidden App Installed on Smartphones*, THE HUFFINGTON POST (Nov. 30, 2011, 12:11 PM), http://www.huffingtonpost.com/2011/11/30/carrier-iq-trevor-eckhart_n_1120727.html.

[7] *See* Larry Greenemeier, *Is Carrier IQ's Data-Logging Phone Software Helpful or a Hacker's Goldmine?*, SCI. AM. (Dec. 3, 2011), http://blogs.scientific american.com/observations/2011/12/03/is-carrier-iqs-data-logging-phone-software-helpful-or-a-hackers-goldmine/. Software of this type is commonly called "rootkit" software, which "is used to gain control over your

weeks following Eckhart's accusation, cell-phone users filed dozens of class action lawsuits claiming that CIQ, wireless carriers, and handset manufacturers intercepted their private electronic communications in violation of the Federal Wiretap Act ("FWA").[8]

While courts agree that electronic communications intercepted by a third party while in flight between the sender and the recipient are within the definition of an illegal interception under the FWA, courts disagree over whether information intercepted before transmission but not technically in flight—like that collected by CIQ—may be covered as well.[9] In the context of the unfolding CIQ litigation, the question becomes: Should courts interpret the FWA to encompass the pre-transit keystroke logging performed by CIQ on behalf of wireless carriers and handset manufacturers?[10]

In short, the answer is yes. Courts that interpret the FWA not to include keylogging[11] rely on an erroneous understanding of the

---

desktop by hiding deep inside your system. Unlike most viruses, it is not directly destructive . . . [but] provide[s] access to all your folders . . . to a remote user." *What is a Rootkit and How it Infects Your PC*, GUIDING TECH (July 19, 2010), http://www.guidingtech.com/4467/what-is-a-rootkit/.

[8] Federal Wiretap Act, 18 U.S.C. §§ 2510–2522 (2006). *See, e.g.*, Complaint at 6, Janek v. Carrier IQ, No. 1:11-cv-08564 (E.D. Mo. filed Dec. 1, 2011), *available at* http://www.docstoc.com/docs/106453596/Class-Action-against-Carrier-IQ_-HTC (filing suit against CIQ for FWA violation).

[9] *Compare* U.S. v. Ropp, 347 F. Supp. 2d 831, 837 (C.D. Cal. 2004) (holding that keylogging interception was not covered under the FWA because the interception did not occur between the sender and recipient, but occurred prior to transfer), *and* U.S. v. Steiger, 318 F.3d 1039, 1050 (11th Cir. 2003) (holding that hacker's acquisition of child pornography stored on defendant's computer did not violate the FWA because the information was not intercepted while in flight), *with* U.S. v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010) (arguing that the FWA covers in flight as well as contemporaneous interceptions that occur immediately after e-mail receipt), *and* Potter v. Havlicek, No. 3:06-cv-211, 2007 WL 539534, at *8 (S.D. Ohio 2007) (arguing that a pre-transit interception could fall within the FWA because it could affect interstate commerce).

[10] 18 U.S.C. § 2511.

[11] "Keylogger" is a shorthand phrase for "keystroke logger." *Definition: Keylogger (Keystroke Logger, Key Logger, or System Monitor)*, SEARCH MIDMARKET SECURITY (May 2004), http://searchmidmarketsecurity.techtarget.com/definition/keylogger.

Act's key terms, disregard analogous situations and technologies that are explicitly covered under the Act, and overemphasize the importance of technical minutiae, resulting in judicial outcomes at odds with the FWA's original purpose.[12] By interpreting the FWA to include keylogging interceptions of pre-transit communications, courts will reach results consistent with both the language and policy goals of the Act, ensuring that privacy protections for modern handset users are commensurate with those originally intended by Congress.

Part II of this Recent Development reviews past scholarly attempts at defining privacy law, generally, while Part III provides an overview of how the CIQ software collects user data and describes several of its allegedly illegal functions. Part IV summarizes the relevant portions of the FWA and reviews various judicial interpretations of the Act as it applies to pre-transit keystroke logging. Part V examines the FWA's structure and legislative history to argue for a broader interpretation of the Act and explores possible outcomes of the CIQ class action suits.

II. DEFINING PRIVACY

On the surface, the CIQ litigation is merely concerned with matters of FWA interpretation—whether "intercept" and "electronic communication" encompass pre-transit keylogging.[13] But from mobile privacy invasions[14] to domestic drone surveillance[15] to GPS tracking,[16] technological progress and

---

[12] *See infra* Part V.A–C.

[13] Federal Wiretap Act, 18 U.S.C. §§ 2510–22.

[14] *See, e.g.*, *iPhone Apps Path and Hipster Offer Address-Book Apology*, BBC (Feb. 9, 2012, 10:13 AM), http://www.bbc.co.uk/news/technology-16962129 (reporting on the apologies issued by two iPhone application makers for uploading user address-book information without express permission).

[15] *See, e.g.*, Chris Kirk, *Domestic Drone Bill Upsets Civil Liberties Advocates*, MEDILL NAT'L SECURITY ZONE (Feb. 10, 2012), http://nationalsecurityzone.org/site/domestic-drone-bill-upsets-civil-liberties-advocates-domestic-drone-bill-upsets-civil-liberties-advocates-domestic-drone-bill-upsets-civil-liberties-advocates/ (noting disagreement over bill that would require FAA to make it easier for law enforcement to use unmanned aircraft).

privacy interests continually prove to be negatively correlated.[17] On a deeper level, therefore, the CIQ litigation is symptomatic of the historically present but increasingly prevalent tension between technology and individual privacy rights.[18]

While identifying that the CIQ litigation implicates privacy concerns is simple, precisely defining the right to privacy is not.[19] There are several reasons for this difficulty. First, the right to privacy is not derived from a single source; tort law,[20] evidence law,[21] property rights,[22] contract law,[23] and constitutional law[24] all

---

[16] *See generally* U.S. v. Jones, 132 S. Ct. 945 (2012) (addressing whether the warrantless use of a GPS tracking device on a motor vehicle constitutes a search under the Fourth Amendment).

[17] In his concurrence, Justice Alito noted the historical tension between technological advances and privacy interests and the resulting effect on the Court's Fourth Amendment jurisprudence:

> [T]he *Katz* test rests on the assumption that [the] hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.

Id. at 10 (Alito, J., concurring).

[18] *Id.*

[19] *See, e.g.*, Lillian R. Bevier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protections*, 4 WM. & MARY BILL RTS. J. 455, 458 (1995) ("Privacy is a chameleon-like word, used denotatively to designate a range of wildly disparate interests—from confidentiality of personal information to reproductive autonomy . . . .").

[20] *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960) (identifying four privacy-related torts).

[21] *See, e.g.*, DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 32 (3d ed. 2008) ("The law of evidence has recognized the importance of protecting the privacy of communications between attorney and client, priest and penitent, husband and wife, physician and patient, and psychotherapist and patient.").

[22] *See, e.g.*, David J. Phillips, *Beyond Privacy: Confronting Locational Surveillance in Wireless Communication*, 8 COMM. L. & POL'Y 1, 21 ("In U.S. legal theory, privacy rights are intimately entwined with rights to access physical spaces.").

contribute to the overall concept of privacy. Second, considering historical scholarly difficulties with defining the right, even if the right to privacy did have a single origin, identifying it likely would not help to sharpen its inherently nebulous contours.[25]

Writing in 1890, Samuel Warren and Louis Brandeis made perhaps the first and most famous attempt at defining the right to privacy. Concerned about privacy invasions resulting from "[i]nstantaneous photographs" and the "newspaper enterprise,"[26] Warren and Brandeis rooted their right to privacy in the common law and conceptualized the right as one protecting individuals from violations of "the 'honor' of another."[27] Over a century later and continuing the attempt to define the boundaries of the right to privacy, leading privacy scholar Daniel Solove characterized the Warren and Brandeis definition as one dealing with "dignitary harms"[28] and identified five other characterizations of the right[29]: (1) the right to control information—the right to exert "control over knowledge about oneself";[30] (2) the right to limit access to the self—the ability to "shield oneself from unwanted access by others";[31] (3) intimacy "both in its relation to identity and . . . to

---

[23] *See, e.g.*, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1251 (1998) (arguing for a default rule for defining how personal information is used but allowing "[t]hose parties for whom the default rule is inefficient" to contract otherwise).

[24] *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 485 (1965) (establishing a fundamental right to privacy).

[25] *See, e.g.*, Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 477–78 (2006) ("Privacy is a concept in disarray. Nobody can articulate what it means.").

[26] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[27] *Id.* at 198.

[28] *See* SOLOVE & SCHWARTZ, *supra* note 21, at 487.

[29] *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1092 (2002) (identifying these major categories).

[30] Charles Fried, *Privacy*, 77 YALE L.J. 475, 483 (1968).

[31] Solove, *supra* note 29, at 1092; *see also* Ruth Gavison, *Privacy and the Limits of the Law*, 89 YALE L.J. 421, 433 (1980) (arguing that the concept of privacy is composed of three "irreducible elements: secrecy, anonymity, and solitude," control over which allows us to control the "extent to which we are known to others").

autonomy";[32] (4) personhood—the right to protect "one's personality, individuality, and dignity";[33] and (5) secrecy—the right to conceal "certain matters from others."[34]

After examining that list, Solove's oxymoronic suggestion that the right to privacy encompasses both everything and nothing begins to make more sense;[35] the characterizations are individually under-inclusive, arguably overbroad in the aggregate, and all overlap.[36] Despite their breadth, several of the above right to privacy categorizations accurately describe the major privacy concerns associated with CIQ-like data collections. Conceiving of privacy as the right to control personal information, the right to limit access to the self, or the right to secrecy all seem applicable in the context of user accusations that CIQ software surreptitiously collects SMS text, phone numbers, and URL information.

Perhaps the easiest way to identify the nature of the privacy interests at stake would be to identify the potential harms caused by the alleged CIQ data collection; the central issue is whether losing the rights to secrecy, to control personal information, or to limit access to the self will injure handset users in any way.[37] Scholars believe that loss of individual control over private data would cause both direct and indirect harm to individuals and society as a whole. First, there is the direct and obvious risk of fraud or identity theft and the resulting financial, dignitary, or physical harm that could follow.[38] Second, a general loss of

---

[32] Tom Gerety, *Redefining Privacy,* 12 HARV. C.R.-C.L. L. REV. 233, 263 (1977).

[33] Solove, *supra* note 29, at 1092.

[34] *Id.*

[35] Solove, *supra* note 25, at 479.

[36] *See* Solove, *supra* note 29, at 1094 ("The conceptions are often too narrow because they fail to include the aspects of life that we typically view as private, and are often too broad because they fail to exclude matters that we do not deem private.").

[37] See *infra* Part V.E for a more specific discussion.

[38] Solove, *supra* note 25, at 488 ("Activities involving a person's information, for example, might create a greater risk of that person being victimized by identify theft or fraud.").

personal control over private data could lead to broader societal " 'architectural' problems"[39]:

> [A] particular activity can upset the balance of social or institutional power in undesirable ways. A particular individual may not be harmed directly, but this balance of power can affect that person's life. The classic example is law enforcement officials having too much power, which can alter the way people engage in their activities. People's behavior might be chilled, making them less likely to attend political rallies or criticize popular views .... Imbalances in power can also be risk enhancing, in that they increase abuses of power.[40]

Regardless of how CIQ's interceptions are characterized and the right to privacy defined, CIQ-like data collections cause dignitary harms when performed without consent and present a clear threat to users' ability to control third party access to their private information.

III. MOBILE ANALYTICS AND CARRIER IQ SOFTWARE

Generally speaking, analytics companies collect, synthesize, and present aggregated user information to their customers to help them reduce maintenance costs, increase revenue, and improve the performance of a particular product.[41] While analytics companies provide usability metrics for a wide array of customers in all industries,[42] mobile analytics companies specialize in providing

---

[39] *Id.* at 487.

[40] *Id.* at 488.

[41] *About Usability*, USABILITY PROF'L ASS'N, http://www.upassoc.org/usability_resources/about_usability/definitions_of_usability.html (last visited Feb. 23, 2012) ("The business benefits of adding usability to a product development process include: [i]ncreased productivity, [i]ncreased sales and revenues, [d]ecreased training alnd support costs, [r]educed development time and costs, [r]educed maintenance costs, [i]ncreased customer satisfaction." (bullet points omitted)).

[42] "Usability really just means making sure that something works well: that a person of average (or even below average) ability and experience can use the thing—whether it's a website, a fighter jet, or a revolving door—for its intended purpose without getting hopelessly frustrated." BOB TULLIS & BILL ALBERT, MEASURING THE USER EXPERIENCE: COLLECTING, ANALYZING AND PRESENTING USABILITY METRICS 4 (2008) (quoting STEVE KRUG, DON'T MAKE ME THINK (2000)). All that is required are "some common themes: A user is involved, [t]hat user is *doing* something, [t]hat user is doing something with a *product, system, or other thing*." *Id.* (bullet points omitted).

solutions specifically tailored for products relating to mobile web and telephone services.[43] For example, application-based analytics companies monitor user crash data for individual handset applications, while mobile web analytics companies collect data relating to mobile handset user webpage views and click behavior.[44]

A. *Carrier IQ, Generally*

CIQ is one of many such mobile analytics companies.[45] It specializes in providing usability data to handset manufacturers and their wireless network operators to ensure proper handset and network performance.[46] Typically, wireless network operators use these data collections to remedy dropped calls, lost SMS messages, or weak network signal strength.[47] Prior to using embedded software to collect performance metrics,[48] carriers and handset manufacturers relied on data from customer surveys, returned products, or customer complaints to diagnose and solve service problems.[49] These processes are cumbersome and unreliable and

---

[43] Madeleine Moss Funes, *The ABCs of Mobile Analytics*, SMART DATA COLLECTIVE (July 21, 2011), http://smartdatacollective.com/brett-stupakevich/38317/abcs-mobile-analytics.

[44] *Id.*

[45] *See Mobile Analytics Providers*, MOBILE STRATEGY, http://m-strat.org/mobile-analytics (last visited Feb. 23, 2012) (providing a compiled list of mobile analytics providers).

[46] *See* Haley Tsukayama, *Who's Using Carrier IQ and for What Purpose?*, WASH. POST (Dec. 1, 2011), http://www.washingtonpost.com/business/technology/whos-using-carrier-iq-and-for-what-purpose/2011/12/01/gIQAGeHpHO_story.html ("Carrier IQ's program is meant to collect user data to 'assist operators and device manufacturers in delivering high-quality products and services to their customers.' "); *Reinvent Customer Care*, CARRIER IQ, http://www.carrieriq.com/reinvent-customer-care/ (last visited Mar. 21, 2012).

[47] *See* Press Release, Carrier IQ, Understanding Carrier IQ Technology *11–*13 (Dec. 15, 2011) *available at* http://www.carrieriq.com/documents/12-december-2011-understanding-carrier-iq-technology/6596/.

[48] "[The] individual measurements on a device, such as signal strength, are called *metrics*." *Id.* at *4.

[49] *See Mobile Intelligence for Network Operators*, CARRIER IQ, http://www.carrieriq.com/network-operators/ (last visited Mar. 21, 2012) ("Sure you can deploy field trucks, use network probes and protocol sniffers, wait for returns, conduct user surveys, or just hope that customers will call in.").

typically involve filling out surveys, questioning disgruntled consumers who are returning products, and collecting and synthesizing general customer oral complaints. Furthermore, these processes rely on customers to recognize problems with their products and effectively communicate them to a company employee before the company can even begin to identify a system-wide solution.[50] CIQ's software improved the efficiency and reliability of problem identification and analysis by offering carriers embedded handset software that automatically provides real-time data directly from user handsets without requiring user participation or knowledge.[51]

Mobile analytic software like CIQ's is vital for handset manufacturers and wireless carriers because it provides them with the ability to accurately determine how their services and devices perform in the real world, to analyze data in real time so wireless carriers can identify and rectify problems immediately, and to work together to improve usability when their products interact.[52] As important as this information is for network operators and manufacturers now, it will only become more valuable in the future as smartphones and tablets grow in both their capabilities and total market share of Internet-connected devices.[53]

---

[50] *Id.* ("[N]one of these [pre-CIQ software] options delivers a clear picture of service quality or the true user experience.").

[51] *Id.* (noting that CIQ "automatically [provides] accurate, real-time data direct from the source—[their] customers' handsets," with "no visible impact to [their] customers"). CIQ sells its software and services to handset manufacturers as well as wireless carriers, but carriers comprise the majority of their clientele. *See* Press Release, Carrier IQ, *supra* note 47, at *2.

[52] *See Reinvent Customer Care*, CARRIER IQ, *supra* note 47.

[53] *See, e.g.*, Diane Mermigas, *Future Growth: It's All About Mobile*, MEDIA POST (Oct. 15, 2010, 5:36 PM), http://www.mediapost.com/publications/article/137796 (describing the "latest data framing the emerging global mobile paradigm that is reinventing consumer orientation for every business in every industry"); CISCO, CISCO VISUAL NETWORKING INDEX: GLOBAL MOBILE DATA TRAFFIC FORECAST UPDATE, 2011–2016 3 (2012), *available at* http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf (predicting that by the end of 2012, there will be more connected mobile devices than people on Earth and that "[g]lobal mobile data traffic will increase 18-fold between 2011 and 2016").

B. *Relationship Between Carrier IQ, Wireless Carriers, and Handset Manufacturers*

Three parties are typically involved in the installation of CIQ's analytics software: CIQ, wireless carriers, and handset manufacturers.[54] First, the carriers purchase CIQ's software, called "IQ Agent,"[55] and specify what profile will best fit their needs.[56] Profiles define the frequency and type of information, or metrics, that will be collected by the IQ Agent and vary depending on the types of performance problems the carrier would like to address.[57] After the profile is defined, CIQ provides installation instructions to the handset manufacturers, who write the software necessary to pass data metrics from the phone to the IQ Agent.[58] Once embedded, the IQ Agent—which "cannot be deleted by consumers through any method provided by Carrier IQ"[59]—is responsible for

---

[54] *See* Press Release, Carrier IQ, *supra* note 47, at *6.

[55] *Id.* at *4. The Carrier IQ software installed on the mobile device is called the IQ Agent. *Id.* The IQ Agent is the first stage in the Network Operator's analytics pipeline and is responsible for identifying, storing, and forwarding diagnostic measurements and data from the handset and the network required to solve network and consumer issues. *Id.* The IQ Agent has been implemented on feature phones, smart phones, data modems, and tablets. *Id.*

[56] *Id.*

[57] *Id.* The press release goes on to explain:

> Each mobile network is different from the others. In order to serve all of those varying needs, Carrier IQ created software that allows Network Operators to create a subset of these metrics (a profile) tailored to solve their individual network requirements. For example, if a Network Operator is interested in understanding the cause of dropped calls, a specific profile can be created to address this issue. That profile is passed to devices loaded with the IQ Agent instructing the devices to provide the Network Operator with *metrics* for dropped-call events. The profile then gathers the associated signaling messages, location, radio conditions and any other essential measurements leading up to the call termination, thus eliminating non-essential data, such as successful call events.

Id.

[58] *Id.* CIQ instructs handset manufacturers on installation specifics by providing them with a "porting guide and a metric requirements specification" that "enables the handset manufacturer to write a software interface to pass the necessary metrics from the handset to the IQ Agent." *Id.* at 6.

[59] *Id.*

sifting through cell phone data and relaying information according to its installed profile.[60] This method, called the "embedded IQ Agent," is the most common method CIQ uses to install its software on user handsets and was the method used to install the CIQ software in Trevor Eckhart's YouTube demonstration.[61]

There are two other methods for installing CIQ on user handsets: the "preload IQ Agent," which differs from the embedded IQ Agent method only because it collects less detailed information,[62] and the "after-market downloadable IQ Agent," which is installed by consumers on their own after they have purchased their mobile device.[63] Of the three, carriers most prefer the embedded IQ Agent—it is pre-installed, collects a more comprehensive dataset than either the preload or after-market IQ Agent, and cannot be deleted by consumers.[64]

In sum, under the embedded method each party has a distinct and necessary role in collecting user data; carriers define the data to be collected, CIQ writes the software to meet these specifications, and handset manufacturers install the software onto "feature phones, smart phones, data modems, and tablets."[65] So while CIQ has been the lightning rod for criticism—and rightly so, since they own the software—manufacturers and wireless carriers also have been sued for directing what information the IQ Agent

---

[60] *Id.* at *4 ("The IQ Agent . . . is responsible for identifying, storing and forwarding diagnostic measurements and data from the handset and the network required to solve network and consumer issues.").

[61] *Id.* at *6; *see Carrier IQ Part #2*, *supra* note 5.

[62] *See* Press Release, CARRIER IQ, *supra* note 47, at *5 (noting that the pre-load IQ Agent "does not require integration by a device manufacturer . . . but the main difference between pre-load and embedded is that the radio diagnostic data . . . are not available for analysis with the pre-load version").

[63] *Id.* at *6 ("In this model, a mobile device user would download the IQ Agent on instruction from Carrier IQ's customer—typically a Network Operator. The metrics available to the downloaded IQ Agent are the same as the pre-load agent.").

[64] *Id.*; *see also Carrier IQ Part #2*, *supra* note 5.

[65] *See* Press Release, Carrier IQ, *supra* note 47, at *4.

should collect, installing the IQ Agent, and using the aggregated data for diagnostic purposes.[66]

C. *Alleged Collection of Improper Data*

Eckhart's YouTube demonstration[67] revealed that the IQ Agent surreptitiously collects more information than seems necessary for network quality control purposes, although CIQ, network operators, and manufacturers disagree as to why.[68] The video begins by highlighting how difficult it is just to find the CIQ application on his HTC handset; it does not appear in the phone's "all applications" list, nor does it appear in the "running applications" list.[69] As noted above, CIQ readily admits that the user cannot remove the embedded IQ Agent.[70] Eckhart shows that not only is the IQ Agent installed and running despite never informing the user of its presence or requesting user consent, but the user is also unable to force-stop the application and prevent it from collecting and relaying data.[71]

In addition to being difficult to discover and impossible to remove, Eckhart demonstrates that the IQ Agent registers keystrokes when the user dials a phone number or performs a Google search, and records the URLs of visited websites and the

---

[66] *See* Complaint, Howell v. Carrier IQ, No. 12CV000157 (D. Minn. Jan. 19, 2012) (filing suit against CIQ, wireless carrier AT&T, and handset manufacturer Apple).

[67] *See Carrier IQ Part #2*, *supra* note 5.

[68] *See* Press Release, Carrier IQ, *supra* 47, at 8. Carrier IQ claims that botched manufacturer software installations are at least partially responsible for these additional collections and notes that the IQ Agent only collects information at the direction of its clients. *See id.*; John Paczkowski, *Carrier IQ Speaks: Our Software Ignores Your Personal Info*, ALL THINGS D (Dec. 1, 2011 4:35 PM), http://allthingsd.com/20111201/carrier-iq-speaks-our-software-monitors-service-messages-ignores-other-data/ (quoting CIQ CEO Larry Lenhart as saying, "It's the operator that determines what data is collected . . . . They make that decision based on their privacy standards and their agreement with their users, and we implement it.").

[69] *See Carrier IQ Part #2*, *supra* note 5.

[70] *See id.* at 6 ("An embedded version of the IQ Agent cannot be deleted by consumers through any method provided by Carrier IQ.").

[71] *Id.*; *see Carrier IQ Part #2*, *supra* note 5.

contents of SMS[72] text messages.[73] Notably, the keystrokes are logged *when typed and prior to user transfer*, and all the information is recorded even when the handset is disconnected from the wireless network.[74]

From a policy perspective, these allegations, if true,[75] are problematic for a number of reasons. First, many users consider embedding this type of software without notice or consent to be, as one commentator called it, "an insane breach of trust."[76] Second, even if CIQ's motives are benign and its "treasure trove"[77] of data kept anonymous, as it claims, any such treasure trove will tempt hackers, advertisers, and law enforcement to find ways to access

---

[72] "SMS stands for 'short message service' . . . [and] is often referred to as texting." Adam Fendelman, *Definition of SMS Text Messaging: What is SMS Messaging, Text Messaging?*, ABOUT.COM, http://cellphones.about.com/od/phoneglossary/g/smstextmessage.htm.

[73] *See Carrier IQ Part #2*, *supra* note 5.

[74] *Id.* The fact that data is collected even when disconnected from the wireless network vitiates the likelihood that CIQ, handset manufacturers, and wireless carriers will successfully fall within an exception to the FWA that permits operators of a wireless communications service to access certain information for quality control and network maintenance purposes. *See* Federal Wiretap Act, 18 U.S.C. § 2511 (2006). Specifically, if a court found that the interceptions were permissible per this exception, the parties could still be liable for any interception that occurred while the handset device was not connected to the wireless network. *Id.*

[75] CIQ has denied nearly all of Eckhart's allegations against the IQ Agent, claiming that its software "does not record, store or transmit the contents of SMS messages, email, photographs, audio or video. For example, we understand whether an SMS was sent accurately, but do not record or transmit the content of the SMS." Phil Nickinson, *Carrier IQ, in a New Press Release, Reminds Us it Works for the Carriers*, ANDROID CENT. (Dec. 1, 2011, 11:07 PM), http://www.androidcentral.com/carrier-iq-new-press-release-reminds-us-it-works-carriers. CIQ has also taken pains to point out that it "acts as an agent for the operators," who determine the diagnostic information that is actually gathered. *Id.*

[76] *The Carrier IQ Cellphone Scandal: "An Insane Breach of Trust,"* THE WK. (Dec. 1, 2011, 6:36 PM), http://theweek.com/article/index/222053/the-carrier-iq-cellphone-scandal-an-insane-breach-of-trust.

[77] David Kravets, *Carrier IQ Admits Holding "Treasure Trove" of Consumer Data, but No Keystrokes*, THREAT LEVEL (Dec. 2, 2011, 8:53 PM), http://www.wired.com/threatlevel/2011/12/carrier-iq-data-vacuum/all/1.

it.[78] Additionally, from a legal perspective, such unauthorized interceptions could violate the FWA, the basics of which are explored in the following section.

IV. INTERPRETING THE FEDERAL WIRETAP ACT

The original purpose of the FWA was to protect the privacy of communications made over a wire from continuing unauthorized surveillance.[79] Congress enacted the Electronic Communications Privacy Act ("ECPA")[80] in 1986, which updated the FWA to prohibit the interception of new electronic communications not contemplated by the original statute. Specifically, the ECPA updated the FWA's provisions to cover "any person who . . . intentionally intercepts . . . any . . . electronic communication."[81] The Act defines "intercept" as "the . . . acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device," and defines "electronic communication" as "any transfer" of information by a "wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[82] The definitions of intercept and electronic communication, then, are linked, and an interception of information might not be an interception under the Act if the communication is determined not to fall within the definition of electronic communication.[83] Since

---

[78] *See infra* section V.E; Bob Brown, *Cornell Prof: Carrier IQ Affair "My Worst Nightmare,"* NETWORK WORLD (Dec. 2, 2011, 10:40 AM), http://www.networkworld.com/news/2011/120211-cornell-carrieriq-253696.html ("How hard would it be to 'de-anonymize' a pile of text messages between me and my wife? . . . Banking IDs with passwords?").

[79] *E.g.*, U.S. v. Councilman (*Councilman II*), 418 F.3d 67, 76 (1st Cir. 2005) (en banc) ("[T]he purpose of the broad definition of electronic storage was to enlarge privacy protections for stored data under the Wiretap Act . . . .").

[80] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510–2522, 2701–2711, 3121–3127 (2006)).

[81] Federal Wiretap Act, 18 U.S.C. § 2511 (2006).

[82] *Id.* § 2510.

[83] *See* U.S. v. Ropp, 347 F. Supp. 2d 831, 833 (C.D. Cal. 2004) (noting that the terms "intercept" and "electronic communication" are "bound up with the jurisdictional element of the statute and requires that the transmission be made by a system that affects interstate commerce").

the ECPA was passed in 1986, the FWA has not received a significant update to Sections 2510 and 2511, the sections addressing interceptions of electronic communications.

The following sections demonstrate that, like those of scholars, judicial interpretations of the FWA's core terms vary widely. Specifically, courts are split as to the proper scope of the FWA's application to pre-transit keylogging.[84] Some courts interpret the FWA narrowly and refuse to cover interceptions other than those made while the communication is in-flight,[85] while others extend the FWA beyond in-flight interceptions.[86]

A. *Narrow Interpretations*

Courts ruling that the FWA does not cover keylogging fall into two main groups: the first is comprised of courts that narrowly interpret the meaning of "interception," while the second group focuses on the meaning of the requirement that the interception occur on a system affecting interstate commerce.

1. *Group One: Narrow Interpretations of Interceptions*

The Eleventh Circuit, drawing on the storage-transit dichotomy[87] to narrowly interpret the meaning of interception,[88]

---

[84] *See supra* note 9; *see also* Jason C. Gavejian, *Keylogging—Jurisdictions at Odds Over Privacy Concerns*, WORKPLACE PRIVACY DATA MGMT. & SECURITY REPORT (May 13, 2010), http://www.workplaceprivacyreport.com/2010/05/articles/workplace-privacy/keyloggingjurisdictions-at-odds-over-privacy-concerns (citing several splits among lower courts).

[85] *See e.g., Ropp*, 347 F. Supp. 2d 831; U.S. v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001).

[86] *See, e.g.*, U.S. v. Szymuszkiewicz, 622 F.3d 701 (7th Cir. 2010); *Councilman II*, 418 F.3d 67 (1st Cir. 2005) (en banc).

[87] The Eleventh Circuit's decision in *United States v. Steiger* highlights what is known as the storage-transit dichotomy. 318 F.3d 1039, 1048 (11th Cir. 2003); *see also* Michael D. Roundy, *The Wiretap Act—Reconcilable Differences: A Framework for Determining the "Interception" of Electronic Communications Following United States v. Councilman's Rejection of the Storage/Transit Dichotomy*, 28 W. NEW. ENG. L. REV. 403, 418–19 (2006) (defining the storage/transit dichotomy to mean that interceptions of stored data are not covered under the FWA, while interceptions of information in transit between sender and recipient are covered). In *Steiger*, a computer hacker gained unauthorized access to the defendant's computer, where he discovered a cache of child pornography that he turned over to police. *Steiger*, 318 F.3d at 1042.

refused to apply the FWA to pre-transit keylogging in *U.S. v. Barrington*.[89] *Barrington* had all the trappings of a bad late '80s movie—a group of fraternity brothers at Florida A&M installed keylogger software on a university registrar computer to record passwords that they later used to change students' failing grades and in-state tuition status.[90] The software recorded keystrokes as they were entered from the keyboard, and there was no evidence that the software captured any information as it was being transmitted beyond the registrar's computer.[91] The court held that the FWA did not apply to this software, ruling instead that the FWA only covers interceptions that are "contemporaneous" with transfer, which it defined as interceptions occurring during interstate transfer or at the moment the information is transmitted beyond the sender's computer.[92]

2. *Group Two: Narrow Interpretations of Systems Affecting Interstate Commerce*

The Central District Court of California's holding in *United States v. Ropp*[93] is an example of a narrow interpretation of the

---

The court ruled that the hacker's acquisition of information stored on the defendant's computer did not violate the FWA because "such unauthorized viewing merely gained access to stored electronic communications." *Id.* at 1050. The court reasoned that "intercept" in the FWA only covered unauthorized acquisition of information that is in transit, not stored. *Id.* Although *Steiger* does not deal with keylogging, the concept of the storage-transit dichotomy is applicable to all FWA cases.

[88] U.S. v. Barrington, 648 F.3d 1178, 1202 (11th Cir. 2011).

[89] *Id.* at 1202–03.

[90] *Id.* at 1183–84. The defendants not only changed their own grades, but also charged others for the service. Matthew Richardson, *Grade Change Scandal*, THE FAMUAN (Mar. 27, 2009, 1:03 AM), http://www.thefamuanonline.com/news/grade-change-scandal-1.1631482#.T0cAt_ES2Ag. Hours after police questioned Barrington, he coordinated a plan to gain access to the registrar system to make further grade changes, which included having some students distract registrar employees while others installed the keyloggers. *Barrington*, 648 F.3d at 1202. Thinking they were in the clear, the group celebrated at Chili's, and continued to make grade changes. *Id.* Their celebration was premature. *Id.*

[91] *Barrington*, 648 F.3d at 1202–03.

[92] *Id.*

[93] 347 F. Supp. 2d 831 (C.D. Cal. 2004).

FWA focusing on the requirement that the communication travel over a system affecting interstate commerce.[94] The defendant in *Ropp* attached an external keystroke logger to the cord running between the sender's keyboard and her personal computer ("PC"), which was linked to the Internet and her company's national network—both interstate systems—at all times.[95] Examining the requirement that the communication be transmitted "in whole or in part by a . . . system that affects interstate commerce,"[96] the court reasoned that the Act only covered interceptions that occur while the communication travels *within* a "system that affects interstate or foreign commerce."[97] It then turned its attention to defining the system in question and the technology used to make this particular interception and decided that, although the PC-to-Internet system is an interstate system within the meaning of the FWA, the interception did not occur there but on the non-interstate keyboard-to-PC "system."[98] Because the court viewed the keyboard-to-PC connection as a separate, non-interstate system rather than as a necessary component part to the PC-to-Internet interstate system,

---

[94] *Id.* at 837–38 ("[T]he Court concludes 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.").

[95] *Id.* at 831.

[96] Federal Wiretap Act, 18 U.S.C. § 2510(12) (2006).

[97] *Ropp*, 347 F. Supp. 2d at 837 ("[T]he communication in question is not an 'electronic communication' . . . because it is not transmitted by a system that affects interstate or foreign commerce."). The defendant argued that, because the keylogger recorded the information before it reached the CPU, the interception was not made simultaneous with a transmission of information affecting interstate commerce, as the Act requires, and therefore was not an "interception" under the Act. *Id.* at 832. The government disagreed, and claimed that the keylogger did violate the FWA because it "literally stripp[ed] communication off a wire as the communication was being transmitted from one point to another." *Id.*

[98] *Id.* at 838. The court also noted that:

> Although this system is connected to a larger system—the network—which affects interstate or foreign commerce, the transmission in issue did not involve that system. The 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.

Id.

the court effectively interpreted keyboard-to-PC keylogging to be outside the purview of the FWA.[99]

The New Jersey District Court similarly interpreted the FWA in *United States v. Scarfo*.[100] Like *Ropp*, *Scarfo* involved a keylogger, but differed in several important ways. First, the keylogger was placed by the Federal Bureau of Investigation (FBI) within the PC itself, not between the keyboard and PC. Second, the keylogger was programmed only to record keystrokes when the computer's modem was disabled, and therefore not connected to the Internet or any other interstate system.[101] Like *Ropp*, the *Scarfo* court held that only interceptions of transmissions made when the communication is traveling *within* an interstate system fell within the FWA.[102] Because the communications were collected by the FBI keylogger when the PC was closed off from the Internet or other interstate connections, the interceptions could not have been made while the information was traveling within an interstate system, and therefore the intercepted communications were not electronic communications for the purposes of the Act.[103]

3. *Summary of Narrow Interpretations*

According to the courts interpreting the statute narrowly via either the interception or interstate system elements, a few requirements for a transmission to be considered an electronic communication become clear. First, the communication must be in flight between point A and point B to be considered intercepted; a file intercepted in storage will not suffice.[104] Second, the in-flight interception must occur as the transmission is moving over a

---

[99] *Id.*

[100] 180 F. Supp. 2d 572 (D.N.J. 2001).

[101] *See id.* at 581–82 ("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 [keylogger] 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.").

[102] *Id.* at 581.

[103] *Id.*

[104] *See* U.S. v. Barrington, 648 F.3d 1178, 1201–02 (11th Cir. 2011); U.S. v. Steiger, 318 F.3d 1039, 1048–51 (11th Cir. 2003).

system affecting interstate commerce, but the message itself need not travel across interstate lines.[105] Finally, systems that may facially appear to be interstate systems—like PCs with an Internet connection—may not be if the interception is found to have been made on a portion of the system that the court considers to be a completely separate system (e.g., the keyboard-PC system in *Ropp*),[106] or if the potentially interstate system is not functioning as an interstate system at the time of the interception.[107]

It is important to introduce several problems with these narrow interpretations, all of which will be discussed in detail in Part V. First, the way in which *Ropp* and *Scarfo* determined that their respective interceptions occurred on a non-interstate system seems contrived: Why did the *Ropp* court decide the keyboard-PC connection was a separate non-interstate system rather than a component part of an interstate system? How can future courts distinguish the two categories? Second, courts like *Barrington* that exclude pre-transit keylogging from the FWA ignore other portions of the FWA that indicate a broader legislative intent.[108] Finally, these narrow interpretations likely would remove Carrier IQ-like keylogging from FWA coverage, resulting in undesirable policies for the consumer public that would undermine individual privacy rights.

B. *Broader Interpretations*

Although not in the keylogging context, other courts have interpreted the FWA more broadly by focusing on the meaning of intercept.[109] In *United States v. Szymuszkiewicz*,[110] the Seventh Circuit implicitly agreed with the *Barrington* court, holding that interceptions under the FWA only covered contemporaneous transfers.[111] Writing for the majority, Judge Easterbrook, however,

---

[105] *See Scarfo*, 180 F. Supp. 2d 572.

[106] *See* U.S. v. Ropp, 347 F. Supp. 2d 831 (C.D. Cal. 2004).

[107] *See Scarfo*, 180 F. Supp. 2d 572.

[108] *See infra* Part V.A, C.

[109] *See, e.g.*, U.S. v. Szymuszkiewicz, 622 F.3d 701 (7th Cir. 2010); *Councilman II*, 418 F.3d 67 (1st Cir. 2005) (en banc).

[110] 622 F.3d 701.

[111] *Id.* at 706.

defined contemporaneous more broadly, arguing that the meaning of " '[c]ontemporaneous' differs from 'in the middle' "[112] and could extend beyond the rigid in-transit timeframe established by opinions like *Barrington*.[113]

The Seventh Circuit's ruling was based at least partially on a previous case that similarly expanded the FWA beyond strict in-transit interceptions: In *United States v. Councilman* (*Councilman II*),[114] the First Circuit addressed the meaning of "intercept" relating to e-mail interceptions.[115] When sent, e-mail messages are split into packets that momentarily pause at various computers while in transit for rerouting.[116] The defendant in *Councilman II* gained unauthorized access to e-mail messages as they were in momentary storage along their route, and claimed that, because the FWA only covers interceptions contemporaneous with transit, his interceptions of the information while in storage were outside the Act's scope.[117] The First Circuit, sitting en banc, rejected this argument and held that certain interceptions of stored information can be considered contemporaneous with transfer and therefore covered under the FWA.[118] *Councilman II* and *Szymuszkiewicz*,

---

[112] *Id.*

[113] Several other courts, like *Barrington*, interpreted "contemporaneous" to mean strictly in-transit. *See* Fraser v. Nationwide Mutual Ins. Co., 352 F.3d 107, 113–14 (3d Cir. 2003); U.S. v. Steiger, 318 F.3d 1039, 1047–49 (11th Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876–78 (9th Cir. 2002); Steve Jackson Games, Inc. v. Secret Service, 36 F.3d 457, 460–62 (5th Cir. 1994).

[114] 418 F.3d 67 (1st Cir. 2005) (en banc). *Councilman II*'s en banc decision reversed *Councilman I*, which held that the FWA did not apply to the interception because it was made while the information was in temporary, split-second storage while in-transit between sender and recipient. U.S. v. Councilman (*Councilman I*), 245 F. Supp. 2d 319, 320–21 (D. Mass 2003), *aff'd*, 373 F.3d 197 (1st Cir. 2004), *vacated*, 418 F.3d 67 (1st Cir. 2005) (en banc).

[115] *Councilman II*, 418 F.3d at 79.

[116] *Id.* at 69.

[117] *Id.* at 72 ("Councilman argues, however, that Congress intended to exclude any communication that is in (even momentary) electronic storage. In his view, 'electronic communications[s]' under the Wiretap Act are limited to communications traveling through wires between computers.").

[118] *Councilman II*, 418 F.3d at 79 ("Councilman's core argument on appeal is that because the messages at issue, when acquired, were in transient electronic

then, represent a distinct break from the narrow interpretations of the *Barrington*, *Ropp*, and *Scarfo* courts, and interpret "contemporaneous" and the FWA to include interceptions made while in temporary storage between sender and recipient and those made just after receipt.

V. ARGUMENT FOR BRINGING PRE-TRANSIT KEYLOGGING WITHIN THE FWA

Although the decisions in *Szymuszkiewicz* and *Councilman II* are distinguishable from the previously mentioned narrow interpretations[119] because they do not apply directly to keylogging, both cases lay the foundation for the argument that the FWA can legitimately apply to interceptions of communications that are not in-transit, depending on whether a court applies—and how it defines—the requirement that an interception be contemporaneous with transfer. A court rejecting the narrow positions could either follow the lead of the First and Seventh Circuits and rely on a contemporaneous interpretation of "intercept" or could argue for inclusion via a broader definition of "interstate system." Regardless of the legal basis for such a decision, a broader interpretation of the FWA has the additional policy benefit of ensuring that interceptions made during handset text composition—a period of time that seems, conceptually, to be a "virtually instantaneous 'conversation[]' more like a telephone call than mail"[120]—are valued and protected similarly to interceptions made while the communication is traveling between sender and recipient.[121]

---

storage, they were not 'electronic communication[s]' and, therefore, section 2511(1)'s prohibition on 'intercept[ion]' of any 'electronic communication' did not apply. That is the argument that we have now rejected . . . .").

[119] *See supra* Part IV.A.1–3.

[120] H.R. REP NO. 99–647, at 22 (1986); *see infra* note 140 and accompanying text.

[121] *See infra* Part V.B. Part V will only examine how courts should interpret the FWA as it relates to CIQ-like interceptions and does not address legislative options. Of course, Congress could remedy CIQ-like data collections legislatively, and, as of this writing, has begun to do so. *See Markey Releases Discussion Draft of Mobile Device Privacy Act in Wake of Carrier IQ Software Concerns*, CONGRESSMAN ED MARKEY, (Jan. 30, 2012),

A. *Using Statutory Structure to Infer Congressional Intent to Cover Certain Stored Content*

As discussed in Part IV.A.1, the *Barrington* court narrowly interpreted the FWA by equating "interception" with "in transit."[122] This position is untenable when the interception requirement is read in context with other portions of the FWA and the Stored Communications Act ("SCA").[123] First, in Section 2510 of the FWA, the definition of "electronic communication" specifically exempts from coverage "electronic funds transfer information *stored* by a financial institution in a communications system used for the *electronic storage and transfer* of funds."[124] Why would Congress need to specifically exempt from coverage a certain type of stored communications if, as *Barrington* held,[125] all interceptions of stored communication fall outside the scope of the FWA? Congress' specific exclusion of stored financial information from

---

http://markey.house.gov/press-release/markey-releases-discussion-draft-mobile-device-privacy-act-wake-carrier-iq-software. In late January 2012, Rep. Ed Mackey released a discussion draft of the Mobile Device Privacy Act, which would require mobile telephone software developers, manufacturers, service providers, and vendors to obtain the user's informed consent prior to installing any mobile analytics software on a user cell phone or selling a cell phone containing such software. *See* Mobile Device Privacy Act, 112th Congress (2012), *available at* http://markey.house.gov/sites/markey.house.gov/files/documents/Mobile%20Device%20Privacy%20Act%20--%20Rep.%20Markey%201-30-12_0.pdf. The legislation as currently proposed, however, inadequately addresses CIQ-like collections. First, the Act only refers to "mobile telephones" and not handsets more generally, and so would exclude tablets and other mobile devices not also used as telephones. *Id.* Second, demanding that network operators obtain informed user consent could, in practice, simply mean another line of fine print added to a user agreement that consumers already ignore. *Id.* Finally, the Act does not restrict what data mobile companies can collect—it just requires that they inform users when they do it. *Id.* The law as currently written, then, would do little to prevent CIQ-like software from continuing to create massive databases of private user information that could be sold or hacked.

[122] *See supra* Part IV.A.1; U.S. v. Barrington, 648 F.3d 1178, 1202 (11th Cir. 2011).

[123] *See infra* notes 124–27 and accompanying text; Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2006).

[124] Federal Wiretap Act, 18 U.S.C. § 2510(12)(D) (2006) (emphasis added).

[125] *Barrington*, 648 F.3d at 1202.

FWA protection evidences its broader intention for the Act to cover both in-transit and stored electronic communications, and therefore *Barrington*'s in-transit restriction is untenable.[126]

Second, the structure and wording of the SCA, which explicitly penalizes unauthorized interceptions of stored electronic information only,[127] also reveal congressional intent to apply the FWA to interceptions of stored communications. Section 2701(c) of the SCA states that the SCA's penalties will not apply where the interception in question has been addressed by Section 2518 of the FWA—the section that outlines procedures for judicial authorization of otherwise illegal interceptions.[128] Like the intra-statute exception found in Section 2510(12)(d), this inter-statute exception suggests that Congress did not intend for the FWA and SCA to cover mutually exclusive types of interceptions—the SCA covering stored only and the FWA covering in-transit only.[129] The *Barrington* assertion that the only interceptions covered in the FWA are those made while the communication is in flight over an interstate system is therefore in direct conflict with the structure of the Act and Congressional intent. By rejecting narrow interpretations, like *Barrington*, and adopting a broader formulation of contemporaneity, courts would bring pre-transit keylogging and other interceptions made outside of interstate transit within the FWA as Congress originally contemplated.

B. *Using "Technical Minutiae" to Interpret Statutes*

Courts with a narrow view of the FWA's requirement that the interception take place on a system affecting interstate commerce typically rely on intricate technical distinctions to interpret the FWA not to include keylogging—like the courts in *Ropp*, which labeled the keyboard-to-PC connection a non-interstate system separate from the PC-to-Internet system, and *Scarfo*, which

---

[126] *See* Roundy, *supra* note 87, at 429 ("If . . . electronic communications in storage could *never* be 'intercepted' under the Wiretap Act, then why would the definition of 'electronic communication' need a specific exclusion for stored financial information?").

[127] Stored Communications Act § 2701.

[128] Federal Wiretap Act § 2518; Stored Communications Act § 2701(c).

[129] *See* Roundy, *supra* note 87, at 429–30.

considered a PC with a functional but temporarily disconnected Internet connection a non-interstate system.[130] This approach is problematic for several reasons. First, because of the difference between the rate at which technologies and judicial precedent advance, basing interpretations of the FWA's provisions entirely on technical minutiae risks creating presently solid precedent that quickly spoils with rapidly changing technological advances.[131]

While relying on technical distinctions whose changes outpace precedential petrification creates numerous problems for courts—particularly lower courts, which could be left with scant guiding precedent[132]—it is perhaps more problematic for criminal defendants. The Fair Warning Doctrine holds that "no man shall be held criminally responsible for conduct which he could not reasonably understand to be proscribed."[133] Because the layperson likely does not understand the inner workings of keylogging software[134] or that their e-mail messages momentarily pause for

---

[130] *See* U.S. v. Ropp, 347 F. Supp. 2d 831 (C.D. Cal. 2004); U.S. v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001); *supra* Part IV.A.2.

[131] *See* Peter V. Roman, *The Black Box Canon of Statutory Interpretation: Why the Courts Should Treat Technology like a Black Box in Interpreting Computer Crime Statutes*, 26 J. MARSHALL J. COMPUTER & INFO. L. 487, 488 (2009) ("[R]apid changes in the underlying technology mean that decisions based on that technology may quickly become obsolete as new technology replaces it."); *see also* Sharona Hoffman & Andy Podgurski, *Securing the HIPAA Security Rule*, 10 J. INTERNET L. 1, 12 (2007) (noting that, because of rapidly changing security technologies, judicial decisions regarding the sufficiency of HIPAA security measures could quickly become antiquated).

[132] *See generally* Stuart Minor Benjamin, *Stepping into the Same River Twice: Rapidly Changing Facts and the Appellate Process*, 78 TEX. L. REV. 269, 283 (noting that "[t]the Supreme Court has expressed agreement with the proposition that changes underlying facts alter the status of the legal conclusions that rely on those facts," and that "changes in relevant facts should prompt a reconsideration of the cases that rely on them").

[133] U.S. v. Harriss, 347 U.S. 612, 617 (1954).

[134] Federal courts require that expert witnesses testify to the technical functionality of keyloggers, indicating that the average keylogger user lacks an in-depth understanding of the technical minutiae on which courts base their FWA interpretations. *See* Roman, *supra* note 131, at 494; *see also* FED. R. EVID. 701–02 (2011).

rerouting while in split-second transit from sender to recipient,[135] and because technological design changes potentially outpace the formation of judicial precedent, a policy of FWA interpretations that is reliant on understanding technical minutiae risks creating a system in which defendants never receive fair warning that their actions potentially violate the FWA.[136]

Second, by relying on specialized technical distinctions not contemplated by Congress when it amended the FWA in 1986, courts risk reaching myopic results that are incompatible with the purposes of the Act.[137] The ECPA was enacted in 1986 to update the FWA, which Congress considered antiquated because it was largely limited to traditional telephone interceptions and did not "address the interception of text, digital or machine communication."[138] Concerned about the pace of technological advancements and their threat to personal privacy,[139] Congress sought to protect "electronic mail," services that "permit an individual to use a keyboard and telephone to transmit electronic messages and data," and other new technologies that are "interactive in nature and can involve *virtually instantaneous*

---

[135] *See Councilman II*, 418 F.3d 67, 69 (1st Cir. 2005) (en banc) (describing the process by which e-mail is transferred).

[136] *See* Roman, *supra* note 131, at 493–94. Supporters of a broadened FWA interpretation might not agree that this is a downside to using narrow factual distinctions to interpret the FWA; if keylogging is intended to be protected, why give hackers affirmative defenses? I include this section about the fair warning doctrine only to support the more general argument that judicial interpretations of the FWA that rely on minute factual distinctions are generally misguided from a statutory interpretation standpoint. That the hacker is sometimes unfairly disadvantaged because of such interpretations does not make the point any less valid, despite the pro-privacy tone of this Recent Development.

[137] *See id.* at 490 ("In ECPA 'electronic storage' cases, the combination of the courts' tendency to delve into the minutiae of technology and the weight of precedent has led to a series of decisions that undermine the purpose of the ECPA and have produced complex and tortured readings of the Wiretap Act.").

[138] H.R. REP. NO. 99-647, at 17 (1986).

[139] *Id.* at 19 ("[I]f Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances." (citations omitted)); *id.* at 20 n.23 (discussing technological advancements that are making cellular service more prone to interceptions).

'conversations' more like a telephone call than mail."[140] Furthermore, the ECPA's legislative history reflects Congress' intention that "electronic communication" should cover "a broad range of communication activities that affect interstate or foreign commerce."[141]

Considering that backdrop, it is easy to recognize that courts like those in *Ropp*, *Scarfo*, and *Barrington* have failed to protect the Act's intent, and should therefore trade in their microscopic focus on technical, factual distinctions for a macroscopic focus on broader policy questions. More specifically, courts should be less concerned about whether a keylogging interception occurs in the moments before transmission of an electronic interstate communication or during the transmission, and more concerned about whether the communication is a "virtually instantaneous 'conversation[]' more like a telephone call than mail" that requires FWA protection.[142]

The First Circuit's treatment of the *Councilman II* case, discussed earlier,[143] provides a blueprint for how this shift should occur in all jurisdictions. Initially, the First Circuit relied on a factual technicality in *Councilman I*, reasoning that, because e-mail in transit from sender to recipient momentarily pauses during transmission for rerouting, any interception made during this split-second "storage" is outside of the scope of the FWA.[144] Rehearing the case en banc, the *Councilman II* court elevated itself above the trees and found the forest; it applied the FWA, holding that the technical in-transit and in-storage *Councilman I* distinction was "inconsistent with Congress' intent."[145]

C. *Cordless Phone Analogy*

Reasonable courts could disagree over the dangers of relying on technical factual distinctions, and there are certainly solid

---

[140] *Id.* at 22 (emphasis added).

[141] *Id.* at 35.

[142] *Id.* at 22.

[143] *See supra*, notes 112–16 and accompanying text.

[144] *See supra*, notes 112–16 and accompanying text.

[145] *Councilman I*, 245 F. Supp. 2d 319, 320–21 (D. Mass. 2003), *aff'd*, 373 F.3d 197 (1st Cir. 2004), *vacated*, 418 F.3d 67 (1st Cir. 2005) (en banc).

counterarguments to the above point that courts should not get bogged down in technical details.[146] But even if courts choose to argue based on technical factual minutiae like the court in *Ropp*, Congress' treatment of cordless phones[147] under the FWA reveals its intent to bring interceptions on similar systems—like pre-transit keylogging on cell phones—within the Act.

Recall that, in *Ropp*, the court held that the keyboard-to-PC connection was a non-interstate system separate from the PC-to-Internet interstate system to which it was connected and, therefore, the keylogging interception that occurred on the keyboard cord did not violate the FWA.[148] Cordless phones present an interesting analogy to this non-interstate-system-within-an-interstate-system theory. A cordless phone operates by converting its user's voice into a radio signal that is transmitted to the phone's base.[149] Under the *Ropp* theory, interceptions of that signal that are made between the handset and the base should not be covered under the FWA because they are made over the handset-to-base system, just like keylogging on the keyboard-to-PC system.[150]

When the ECPA was first enacted, cordless phones were explicitly exempt from coverage because radio signals were so easily intercepted that Congress considered cordless phone users not to have a reasonable expectation of privacy.[151] The rationale

---

[146] *See, e.g., Councilman II*, 418 F.3d 67, 84 (1st Cir. 2005) (en banc) (arguing that the Fair Warning Doctrine did not apply to the e-mail interpretation in question because "[o]ne must apply tools of statutory construction to *remove* the conduct from the statute's ambit by interpreting a subtlety in the definition of 'wire communications.' ").

[147] "Cordless phone" does not refer to cell phones, which are, of course, cordless. In this context, a cordless phone is one that operates within a limited range around its base, which itself is connected to a telephone wire. *See* H.R. REP. NO. 103-827, at 30 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3510 (using this definition of a cordless phone).

[148] *See supra* Part IV.A.2.

[149] *See* H.R. REP. NO. 99-647, at 33 (1986) (describing the cordless phone technology referred to in the Act).

[150] *See supra* Part IV.A.2.

[151] H.R. REP. NO. 99-647, at 33 ("Because the communications made on some cordless telephones can easily be intercepted with readily available technologies (such as AM radio), it would be inappropriate to make such interception a criminal offense.").

for exclusion, then, was completely unrelated to the *Ropp* non-interstate system theory.[152] In fact, once cordless phone technology improved and could scramble radio signals traveling between the handset and base,[153] Congress removed the ECPA's cordless phone exception by explicitly stating that the FWA "now applies to the interception of conversations over . . . cordless phones."[154] Congress' inclusion of cordless phone interceptions directly addresses narrow, *Ropp*-like, system-within-a-system interpretations, revealing that Congress did not intend for such technical distinctions to preclude coverage of pre-transit interceptions between sender and recipient over an interstate system.

D. *Narrow and Broad Interpretations Applied to CIQ*

Assuming that the IQ Agent records keystrokes,[155] such as phone numbers and text messages, prior to interstate transmission, courts could come to very different conclusions depending on which interpretation of "affecting interstate commerce" and "interception" they apply. A court applying the *Scarfo-Ropp* non-interstate-system-within-an-interstate-system approach would likely find that the IQ Agent's interceptions do not fall within the FWA because the interceptions occur at the time the keypad registers the keystrokes. Such a court would hold that the keypad-to-handset non-interstate system on which the interceptions were made is distinct from the sender-handset-to-recipient-handset

---

[152] *Id.*

[153] *See* Basil W. Mangano, *The Communications Assistance for Law Enforcement Act and Protection of Cordless Telephone Communications: The Use of Technology as a Guide to Privacy*, 44 CLEV. ST. L. REV. 99, 119–20 (1996) ("Congress' willingness to protect cordless phones appears to have come only after those phones were equipped with anti-interception devices.").

[154] Bartnicki v. Vopper, 532 U.S. 514, 524 (2001); *see* H.R. REP. NO. 103-827, at 10 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3490 ("The protections of the Electronic Communications Privacy Act of 1986 are extended to cordless phones . . . .").

[155] CIQ is accused of doing much more, such as viewing the content of SMS messages within a recipient's handset prior to being seen by the recipient. *See Carrier IQ Part #2*, *supra* note 5. However, this paper is only focused on the pre-transit interception of keystrokes and not any in-transit interceptions CIQ may have made.

interstate transit system, and therefore falls outside the Act. Similarly, a court applying a *Barrington*-style narrow interpretation would look at the timing of the interception and ask whether it was contemporaneous with transfer. Because these courts define "contemporaneous with transfer" exclusively to mean interceptions of information in flight between sender and recipient,[156] such a court would likely find that the IQ Agent's pre-transit keylogging falls outside the FWA.

For the reasons listed above,[157] courts should take a broader, *Szymuszkiewicz*- or *Councilman II*-like point of view in the CIQ context. Such a court would have the same starting point as a *Barrington* court—Was the interception contemporaneous with transfer?—but would be more willing to interpret "contemporaneous" to apply to interceptions made outside of the path between the sender's cell phone and the information's recipient, just as *Szymuszkiewicz* and *Councilman II* interpreted the Act in an e-mail context.[158] Such a decision would not only fulfill the original purpose of the Act, inferred from the stored financial information provision and Congress' express coverage of cordless phone interceptions, but would also result in beneficial privacy protections and policy outcomes for hundreds of millions of handset users.

E. *Policy Benefits*

In addition to the legal justifications for why the FWA should cover pre-transit keylogging, there are specific policy benefits that would result from bringing CIQ-like software within the Act. First, CIQ's IQ Agent has collected a "treasure trove"[159] of handset user data that has raised fundamental privacy concerns about who might be capable of accessing it. Even if the software "does exactly what [CIQ] say[s] . . . no call logging, no text logging, no URL recording" and just performs harmless diagnostics, the software still creates an enormous dataset that third parties might

---

[156] *See* cases cited *supra* Part IV.A.1–2.
[157] *See* discussion *supra* Part V.A–C.
[158] *See* discussion *supra* Part IV.B.
[159] Kravets, *supra* note 77.

be tempted to access.[160] Advertisers, for example, would certainly be interested in accessing information regarding the times of day and locations that users visit certain webpages or when they activate and deactivate certain mobile applications, all of which could be sold as valuable market research.[161]

In addition to advertisers, law enforcement agencies have an interest in acquiring this information as part of criminal investigations—and the interest is more than theoretical. The FBI recently turned down a Freedom of Information Act ("FOIA") request for any manuals, documents, or other written guidance used to access or analyze data gathered by programs developed or deployed by CIQ."[162] The FBI denied the request not because they lack related documentation, but because the information they do possess is subject to a FOIA exception covering materials that, if disclosed, could interfere with an ongoing investigation.[163] This could mean that the FBI has already developed a method for accessing CIQ data and has utilized it, or plans to utilize it, in a

---

[160] Dennis Fisher, *With Mobile Devices, Users are the Product, Not the Buyer*, THREAT POST (Dec. 7, 2011, 3:33 PM), http://threatpost.com/en_us/blogs/mobile-devices-users-are-product-not-buyer-120711 (noting that in addition to performing "simple diagnostics . . . it's also creating a trove of information on each user's interactions with the device and sending it off to the carrier. That data would be quite valuable in some cases to attackers—or even advertisers—who might like to know what Web pages a person is visiting, where he's located at a given moment or who he's texting.").

[161] *See* Kevin Fitchard, *Is Carrier IQ Making You Your Operator's Lab Rat?*, GIGAOM (Dec. 13, 2011, 10:03 AM), http://gigaom.com/mobile/is-carrier-iq-making-you-your-operators-lab-rat. Fitchard explained the draw for advertisers:

> So if an operator wanted to test the viability of a new social media data plan, it could track how often a subset of its customers access sites or apps like Twitter or Facebook versus communicating via SMS. The operators have a lot of demographic data about their customers, which they could easily marry to the near-real-time device and network information it collects from IQ Agents. There's a potential market research bonanza buried in that app.

Id.

[162] *See* Michael Morisy, *FBI: Carrier IQ Files Used for "Law Enforcement Purposes,"* MUCKROCK (Dec. 12, 2011, 2:30 PM), http://www.muckrock.com/news/archives/2011/dec/12/fbi-carrier-iq-files-used-law-enforcement-purposes/.

[163] *Id.*

current investigation.[164] Couple this possibility with a recent California Supreme Court holding that police may, without a warrant, search an arrestee's cell phone while he is in police custody,[165] and there is a real, near-future possibility that arrests could routinely be accompanied by a police search of databases of unauthorized handset user data.[166]

The technology behind CIQ-style mass keylogging has developed beyond that used in single-victim cases like *Ropp*, *Scarfo*, and *Barrington*, in which the narrow interpretations of the FWA developed and is arguably much more dangerous simply due to the scale of the operation.[167] As the public risk increases, so should the punishment, and the FWA provides perhaps the stiffest punishments of the possible federal statutes into which keylogging might fall.[168] For example, the FWA permits harsher civil

---

[164] Alternatively, invoking the exception could mean that the FBI is investigating CIQ itself, not individual handset users. *See* Mike Masnick, *FBI Admits That it Uses Carrier IQ for Law Enforcement Purposes; Won't Say How*, TECH DIRT (Dec. 13, 2011, 12:06 PM), http://www.techdirt.com/blog/wireless/articles/20111213/00271717060/fbi-admits-that-it-uses-carrier-iq-law-enforcement-purposes-wont-say-how.shtml.

[165] *See* People v. Diaz, 244 P.3d 501, 506 (Cal. 2011) (holding that police search of defendants cell phone within ninety minutes of arrest did not violate the Fourth Amendment because of "reduced expectations of privacy caused by the arrest" (quoting U.S. v. Chadwick, 433 U.S. 1, 20–21 (1977)).

[166] *See, e.g.*, Greenemeier, *supra* note 7 ("The notion that spy agencies or law enforcement could take advantage of Carrier IQ to access private information is particularly relevant given the California Supreme Court case earlier this year that awarded police the authority to search mobile phones without a warrant.").

[167] *See supra* note 2 and accompanying text.

[168] The FWA provides for penalties of $100 per day or $10,000 per violation. Federal Wiretap Act, 18 U.S.C. § 2522 (2006); *see also* Barry Levine, *Fallout Continues for Carrier IQ Tracking Software*, NEWSFACTOR (Dec. 2, 2011, 3:53 PM), http://www.newsfactor.com/story.xhtml?story_id=81225&full_skip=1. The Stored Communications Act awards damages and recuperation of profits, but requires that plaintiff show actual damages. Stored Communications Act, 18 U.S.C. § 2707 (2006); Van Alstyne v. Elec. Scriptorium, 560 F.3d 199, 208 (4th Cir. 2008) (holding that plaintiff must show actual damages to recover under the Stored Communications Act). The Pen Register Act calls for unspecified fines or imprisonment for less than one year. Pen Register Act, 18 U.S.C. §§ 3121–3127 (2006). The Computer Fraud and Abuse Act provides for an unspecified fine and five or ten years imprisonment, but only if the act caused a loss

penalties—"up to $10,000 per day for each day in violation"—than the SCA.[169] By adopting a broader standard and bringing pre-transit keylogging firmly within the FWA, the result will be a more effective deterrent for this type of mass data collection.

Using a narrow interpretation to exclude CIQ-like keylogging from the FWA would also create some odd incentives for potential hackers. Because there are few discernible differences, in effect, between pre-transit keylogging and in-transit interception—for example, both occur instantly and only moments apart chronologically—it makes little sense to punish in-transit interceptions more harshly under the FWA than pre-transit interceptions under, for example, the SCA.[170] Somewhat ironically, pre-transit stored communications, not in-transit communications, are "most vulnerable to unlawful acquisition"[171] because the necessary devices are often easy to use and inexpensive to purchase off the shelf.[172] Applying the FWA's stiff penalties to pre-transit keylogging will therefore have the benefit of creating appropriate deterrents for would-be hackers.

Finally, there is currently some confusion among courts and commentators about which statute covers this type of

---

exceeding $5,000. *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006).

[169] *See* Andrew R. Schulman, *What Civil Practitioners Should Know About the Federal Wiretap and Stored Communications Act* (Nov. 11, 2011), *available at* http://www.andrewschulman.com/Briefs/cle%20wiretap.PDF ("The Stored Communications Act permits the same types of relief as the Wiretap Act, except that statutory damages are limited to $1,000.").

[170] Thomas P. Ludwig, Casenote, *What Online Activity Does the Wiretap Act Protect? The Ninth Circuit Holds that Unauthorized Access of a Secure Website Does Not Violate the Federal Wiretap Act:* Konop v. Hawaiian Airlines, Inc., 7 COMPUTER. L. REV. & TECH. J. 301, 308 (2002–2003) (noting that a definition of "intercept" bringing keystroke logging within the FWA "avoids the situation in which a hacker or similarly unauthorized party can circumvent the harsher penalties of the Wiretap Act by simply waiting to acquire the contents of an electronic communication until it rests either permanently or temporarily in electronic storage . . . .").

[171] *Id.*

[172] *See, e.g.*, Roundy, *supra* note 87, at 403–04 (noting that pre-transit interceptions are normally easier, cheaper, and more efficient than interceptions made while the communication is in transit between sender and recipient).

keylogging[173]: the SCA,[174] the Computer Fraud and Abuse Act,[175] the Pen Register Act,[176] or the FWA.[177] By narrowly interpreting the FWA, courts exacerbate the problem by removing the FWA as a potential sanctuary for keylogging claims. An interpretation that ignores the hyper-technical distinctions between interstate systems and their sub-systems would provide a statutory home within the FWA for keylogging that is currently nonexistent.

---

[173] Paul Koob, Comment, *Not Enough Fingers in the Dam: A Call for Federal Regulation of Keyloggers*, 28 TEMP. J. SCI. TECH. & ENVTL. L. 125, 127–28 (2009); *see also* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1617 (2003) (noting that there are few available decisions interpreting portions of computer misuse statutes, and even these "reflect a diverse range of possible approaches").

[174] 18 U.S.C. § 2701 (2006).

[175] 18 U.S.C. § 1030.

[176] 18 U.S.C. §§ 3121–3127.

[177] 18 U.S.C. §§ 2510–2522. At least one commentator has noted how keylogging has failed to find a sufficient home within federal surveillance legislation:

> [T]he Computer Fraud and Abuse Act, despite its most recent amendments, has significant private enforceability issues that weaken its potential power to combat the problems of keystroke loggers. Other federal statutes pertaining to surveillance exist, but these other components of the current legal landscape are insufficient to effectively alleviate the problems associated with keylogging devices. The current federal surveillance legislation also includes the Electronic Communications Protection Act .... [but] [d]ue to various courts' statutory interpretations of these provisions, many individuals who use keylogging devices and software can escape liability, falling outside the range of current federal legislation.

Koob, *supra* note 173, at 127–28. The Computer Fraud and Abuse Act, for example, requires the plaintiff to prove damages in excess of $5,000, and some courts require an additional showing of a service interruption. *Id.* Therefore, "the [Computer Fraud and Abuse Act] creates barriers for private plaintiffs attempting to assert claims against individuals who have used keylogging software ...." *Id.* at 135. *See generally* Sagi Schwartzberg, *Hacking the Fourth: How the Gaps in the Law and Fourth Amendment Jurisprudence Leave the Right to Privacy at Risk*, 30 U. LA VERNE L. REV. 467 (2009) (discussing various gaps in privacy law, including the conflict between technological advancement and the constitutional right to privacy).

VI. CONCLUSION

CIQ's IQ Agent software poses unique and substantial threats to handset user privacy. Viewed historically, the litigation is symptomatic of the broader tension between the inevitability of technological advancement and the desire for individual control over private information. Several courts, including those in *Ropp*, *Scarfo*, and *Barrington*, have created misguided FWA precedents that are inconsistent with congressional intent to protect continual interceptions of pre-transit electronic communications that are conceptually part of the communications process. By abandoning narrow judicial interpretations of the FWA and, instead, interpreting the Act broadly, courts would remain true to the statute's original purpose, reach desirable policy outcomes, and help to sharpen our modern understanding of individual privacy rights.