THE KATZ OUTTA THE BAG:

BRINGING NATIONAL SECURITY LETTERS INTO COMPLIANCE WITH THE "REASONABLE EXPECTATION OF PRIVACY" TEST

Anees Mokhiber*

The Electronic Communications Privacy Act of 1986 ("ECPA") equips the FBI with the power to issue National Security Letters ("NSLs"). The language of the ECPA, however, contemplates an era of electronic communication long since passed. Electronic communication has transformed rapidly with the evolution of computer technology. At present, the outdated form of the ECPA allows the FBI to utilize NSLs to retrieve information in a manner which runs afoul of Fourth Amendment privacy protections. Accordingly, this Comment proposes to amend the ECPA to account for the ongoing evolution of computer technology which powers the transmittal of electronic communications in the modern age. Additionally, this Comment calls for a commitment to legislative adaptability, to ensure that any statute governing electronic communications is up to date with its subject matter. The goal of these proposed amendments is to tighten the investigative scope of NSLs, and ensure the United States citizen of her reasonable expectation of privacy from unreasonable searches and seizures.

* Antonin Scalia Law School, George Mason University, J.D., May 2017; George Mason University, B.S., 2014. Sincere and special thanks to my friends and family who commented and reviewed this Comment many more times than they would have liked to.

INTRODUCTION

Imagine you were hired as the General Counsel for Facebook in early March 2014. Your employer is the gold standard in the social networking arena. Having recently acquired its most up-and-coming competitors, such as Instagram and WhatsApp, your employer now owns a myriad of social media applications that provide diverse messaging and information sharing features.[1] Consequently, Facebook faces a bevy of nuanced emerging legal issues that ultimately fall on your desk. When hiring you, Facebook made it unambiguous that you must uphold the privacy interests of its users in the administration of your duties as General Counsel.

Although you have never practiced law for a social networking service ("SNS") before, you are cognizant of the

[1] *See generally* Caitlin McGarry, *How Facebook Messenger, Instagram, and WhatsApp Coexist Under Facebook*, MACWORLD (Mar. 26, 2015, 11:00 AM), http://www.macworld.com/article/2902226/how-facebook-messenger-instagram-and-whatsapp-coexist-under-facebook.html.

emerging privacy concerns of individuals who use social networking applications. In fact, upon graduating from law school, you clerked for the late Justice Antonin Scalia, a self-styled defender of Fourth Amendment privacy interests. In your time shadowing Justice Scalia, you were steeped in the rich considerations of individual protections against unreasonable government searches and seizures. You were thrilled to accept this new position, especially for the opportunities that this post could provide to defend the civil liberties of Facebook, Instagram, and WhatsApp patrons.

After a month on the job, you receive a package from the Federal Bureau of Investigation ("FBI"). Inside the package is a National Security Letter ("NSL"). The NSL seeks to compel the disclosure of "subscriber information and toll billing records, or electronic communication transactional records" ("non-content information"), such as logs of the time, participants, and duration of certain WhatsApp conversations.[2] The FBI claims that the records sought are "relevant to an authorized foreign counterintelligence investigation."[3]

After reviewing Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"), you conclude that this NSL complies with 18 U.S.C. § 2709 ("Section 2709").[4] Nevertheless, you feel conflicted between your newfound sense of duty to protect against privacy infringements and your legal duty to comply with a lawful FBI NSL. Additionally, you are not certain that the non-content information sought by this NSL can be disclosed to the FBI without inadvertently disclosing information that is protected by the Fourth Amendment ("content information"). Ultimately, despite your sense of obligation to protect the privacy interests of your employer's patrons and your belief that compliance with the NSL may run afoul of the Fourth Amendment, you comply with the NSL to play it safe. After all, your job is not to decide whether Congressional legislation ought to be followed.

---

[2] 18 U.S.C. § 2709(a) (2015).
[3] 18 U.S.C. § 2709(b)(1) (2015).
[4] *See* 18 U.S.C. §§ 2701-2712 (2015).

Given the current form of the ECPA, the situation described above, although ominous, presents a plausible sequence of events for a third party SNS, such as Facebook or Google, which offers social media applications ("Apps"). The ECPA, and Section 2709 in particular, allow the FBI to issue NSLs with neither judicial approval nor a showing of probable cause.[5] The rationale is that a duly issued NSL can only compel the disclosure of non-content information, which, in contrast to content information, is unprotected by the Fourth Amendment.[6]

However, the Apps used by individuals to communicate both non-content and content information are evolving alongside the computers that contain them.[7] As the technology behind Apps has grown more complex, the boundary between content and non-content information has become murkier.[8] This evolution of technology is incessant, notwithstanding the stagnation of the statutory authority that governs it.[9] To adequately protect the privacy interests of App users, amendments must be made to the statutes that authorize the issuance of NSLs upon a SNS. To ensure the FBI cannot obtain Fourth Amendment protected information through the issuance of a NSL, Congress must bring the ECPA up-to-speed with its subject matter.

Part I of this Comment sketches the evolution of both computer and App technology, to establish the technological landscape that the relevant statutes must govern. Part II provides an overview of the four main statutes that authorize the FBI to issue NSLs, drawing specific attention to the ECPA and Section 2709. Part III acknowledges the troublesome Fourth Amendment implications that may arise from the issuance of

---

[5] *See* 18 U.S.C. § 2709(a)-(g) (2015).
[6] *See generally* 18 U.S.C. § 2709(b)(1)-(2) (2015).
[7] *See generally* Melvin Wilson, *Messaging Apps: The New Face of Social Media and What it Means for Brands*, IPG MEDIA LAB 1, 7-9 (2014), https://ipglab.com/wp-content/uploads/2014/04/MessagingApps_Whitepaper_Final.pdf.
[8] NAT'L ASS'N OF CRIM. DEF. LAW., ELECTRONIC SURVEILLANCE & GOVERNMENT ACCESS TO THIRD PARTY RECORDS 6 (2012), https://www.nacdl.org/reports/thirdparty records/thirdpartyrecords_pdf.
[9] *Id.* at 1.

NSLs, hypothetically applying the *Katz v. United States* reasonable expectation of privacy test and discussing the hazards that may arise from the potential inseparability of content and non-content information. Part III also argues that the current legislation on NSLs leaves citizens vulnerable to violations of the Fourth Amendment by the FBI. Part IV provides recommendations with both a short-term and long-term outlook. First, looking to the immediate needs of citizens, Part IV proposes a set of amendments to the ECPA. Second, with an eye to the long-term preservation of constitutional protections, Part IV calls for a commitment to legislative adaptability in light of the foreseeable evolution of the computer and App technologies that are amenable to the issuance of NSLs. The purpose of this Comment is to offer amendments that adjust the NSL process such that the government can maintain the viability of NSLs as an investigative tool while remaining compliant with the Fourth Amendment of the Constitution.

I. THE EVOLUTION OF COMPUTER AND APP TECHNOLOGY

In 1975, Intel founder Gordon Moore prophesied that "the number of transistors incorporated in a [computer] chip would approximately double every 24 months" ("Moore's Law").[10] In layperson's terms, Moore predicted computer power would double every two years.[11] To put Moore's Law into empirical perspective, consider that modern handheld microcomputers, such as the Apple iPad 2, offer computing capabilities on par with the Cray 2 supercomputer, which was the world's fastest computer just three decades ago.[12] Similarly, today's average smartphone, such as the iPhone 5, operates with computing power greater than the computer that took Apollo 11 to the moon.[13] While such rapid development in computer

[10] Thomas L. Friedman, *Moore's Law Turns 50*, N.Y. TIMES (May 13, 2015), http://www.nytimes.com/2015/05/13/opinion/thomas-friedman-moores-law-turns-50.html?_r=0.

[11] *Id.*

[12] Billy Clayton, *There's a Supercomputer in Your Pocket*, U. MICH. ENG'G (Feb. 28, 2013), http://dme.engin.umich.edu/mightymobile.

[13] Ronald A. Cass, *Article, Lessons from the Smartphone Wars: Patent Litigants, Patent Quality, and Software*, 16 MINN. J. L. SCI. & TECH. 1, 13 n.49 (2015).

technology within a relatively short timeframe may appear unfathomable, this accelerated pace of computer development was long anticipated.[14]

Moore's Law proved true for the better part of five decades and finds supporting evidence in the steady progression of processing and storage capacities of modern computers.[15] Put plainly, computer technology has advanced exponentially since the mid-twentieth century, and little reason exists to expect anything other than a trajectory of indefinite, continued growth at a similar rate.[16]

This evolution in computer technology has been accompanied by the emergence of SNSs.[17] Cumulatively, SNSs provide millions of Apps that any individual with an average smartphone may access.[18] Through Apps, hundreds of millions of United States citizens maintain instant hand-held communication.[19] Consequently, phone calls are no longer the primary medium through which individuals communicate.[20] Apps provide a range of photo, video, message, and other multimedia sharing faculties utilized by smartphone users on a daily basis.[21] Collectively, Apps such as Facebook, Instagram,

[14] *Id.*; Arnold Thackray, David C. Brock & Rachel Jones, *Fateful Phone Call Spawned Moore's Law*, SCI. AM. (Apr. 17, 2015), https://www.scientificamerican.com/ article/ fateful-phone-call-spawned-moore-s-law-excerpt.

[15] Bret Swanson, *Moore's Law at 50: The Performance and Prospects of the Exponential Economy*, AM. ENTER. INST. 1 (Nov. 2015), https://www.aei.org/wp-content/uploads/2015/11/Moores-law-at-50.pdf.

[16] Natalie Wolchover, *What is the Future of Computers?*, LIVE SCI. (Sept. 10, 2012), http://www.livescience.com/23074-future-computers.html.

[17] *Mobile Telecommunications: Telecom Technology Evolution*, TATA CONSULTANCY SERVS., http://sites.tcs.com/insights/perspectives/enterprise-mobility-telecommunications-telecom-technology-evolution (last visited Nov. 4, 2016) [hereinafter TATA CONSULTANCY SERVS.].

[18] *See* STATISTA, *Statistics and Facts About Mobile App Usage*, https://www.statista.com/topics/1002/mobile-app-usage (last visited Jan. 1, 2017).

[19] *See* STATISTA, *Statistics and Facts About Social Networks*, https://www.statista.com/ topics/1164/social-networks (last visited Jan. 1, 2017).

[20] TATA CONSULTANCY SERVS., *supra* note 17.

[21] *Id.*

WhatsApp, among others, have equipped hundreds of millions of citizens with the opportunity to convey messages instantly. SNSs store these communications in their regular course of business.[22]

This Comment's analysis of the evolution of computer and App technology dates only as far back as 1986. This timeframe allows strictly for an analysis of the evolution that has taken place since the enactment of the ECPA and Section 2709.[23]

A. The Evolution of Computer Technology

In contemplating the evolution of computer technology, specifically the development of storage capacities and processing speeds, this Comment exclusively uses a set of computer models produced by Apple, Inc. ("Apple") as its case study.

In 1986, Apple released the Mac Plus ("1986 Model"), which featured a maximum storage capacity of one megabyte and a processor speed of eight megahertz.[24] In 1990, Apple released the Macintosh IIfx ("1990 Model"), which offered a maximum storage capacity of 128 megabytes and a processing speed of 40 megahertz.[25] In 2000, Apple released the iMac G3/350 ("2000 Model"), which offered a maximum storage capacity of seven gigabytes and a processing speed of 350 megahertz.[26] In 2010, Apple released a cellular phone, the iPhone 4 ("2010 Model"), which offered a maximum storage capacity of 32 gigabytes and a processor speed of one

---

[22] *Mobile Messaging and Social Media 2015*, PEW RES. CTR. (Aug. 19, 2015), http://www.pewinternet.org/2015/08/19/mobile-messaging-and-social-media-2015; *Mandatory Data Retention*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/mandatory-data-retention (last visited Nov. 4, 2016).

[23] *See generally* 18 U.S.C. § 2709 (2015).

[24] *Apple Macintosh Plus (ED) Specs*, EVERYMAC (Apr. 7, 2017), http://www.everymac.com/systems/apple/mac_classic/specs/mac_plus.html.

[25] *Apple Macintosh IIfx Specs*, EVERYMAC (Apr. 7, 2017), http://www.everymac.com/systems/apple/mac_ii/specs/mac_iifx.html.

[26] *Apple iMac G3/350 (Summer 2000 - Indigo) Specs*, EVERYMAC (Apr. 7, 2017), http://www.everymac.com/systems/apple/imac/specs/imac_350_indigo.html.

gigahertz.[27] Most recently, in 2016, Apple released its newest product, the iPhone 7 Plus ("2016 Model").[28] This 2016 Model, although a cell phone, has computer capabilities that surpass decades of Apple laptops and desktops.[29] The 2016 Model offers a maximum storage capacity of 256 gigabytes and a processing speed of approximately 2.4 gigahertz.[30]

For a quantifiable perspective, consider that in terms of storage capacity, the 2016 Model offers 256 thousand times more storage than the 1986 Model, two thousand times more storage than the 1990 Model, 36.57 times more storage than the 2000 Model, and eight times more storage than the 2010 Model.[31] Regarding processing capabilities, the 2016 Model offers processing speeds 2.4 times faster than the 2010 Model, 4.8 times faster than the 2000 Model, 60 times faster than the 1990 Model, and 300 times faster than the 1986 Model.[32]

As evidenced by these statistics, the entire concept of a "computer" has taken on a more nuanced definition since 1986.[33] In 2016, a state of the art "computer" can be effortlessly carried on one's person, while still providing functionality greater than that of a 5,500-pound supercomputer from less than three decades ago.[34] However, despite the fact that the designs of

---

[27] *Apple Iphone 4 (16,32 GB Specs)*, EVERYMAC (Apr. 7, 2017), http://www.everymac.com/systems/apple/iphone/specs/apple-iphone-4-specs.html.
[28] *Compare iPhone Models*, APPLE, INC., http://www.apple.com/iphone/compare (last visited Oct. 14, 2016) [hereinafter APPLE].
[29] *Id.*
[30] *Id.*; *iPhone 7 to Feature Up to 3 GB of RAM, 2.4 GHz A10 Processor, Water-resistance, New Colors*, PHONEARENA (Sept. 3, 2016), http://www.phonearena.com/news/iPhone-7-to-feature-up-to-3-GB-of-RAM-2.4-GHz-A10-processor-water-resistance-new-colors_id84945 [hereinafter PHONEARENA].
[31] *Compare iPhone Models*, APPLE, http://www.apple.com/iphone/compare (last visited Oct. 14, 2016).
[32] PHONEARENA, *supra* note 30.
[33] *See* Swanson, *supra* note 15, at 3-4.
[34] *Compare iPhone Models*, APPLE, http://www.apple.com/iphone/compare (last visited Oct. 14, 2016); *The Cray-2 Series of Computer Systems,* CRAY RES., INC. 5 (1988), http://www.craysupercomputers.com/downloads/Cray2/

computers have diversified and the capabilities of computers have multiplied, the legislation that governs the FBI's permissible investigative scope into computers, and the information contained within Apps remains unchanged.[35] The lack of legislative adaptation grows all the more concerning in light of the simultaneous evolution of App technology that has accompanied the evolution of computer technology.[36]

B. The Evolution of App Technology

To provide an organized presentation of the evolution of App technology, this subsection is bifurcated between analysis on a macro- and micro-level. The macro-level analysis covers the growth of Apps broadly, specifically addressing how emergent SNSs have provided increased App availability resulting in a drastic expansion of App usage since 1986. The purpose of the macro analysis is to quantitatively demonstrate how much more prevalent SNSs and Apps have become since the enactment of the ECPA and Section 2709.

The micro-level analysis narrows its focus to Facebook in particular. This analysis discusses the growth in the development of the capabilities and functions of such Apps since 1986. The purpose of this micro analysis is not just to reveal the sheer increase in the total number of App users, but also to qualitatively demonstrate the wealth of information that App users are now capable of sharing and transmitting since the enactment of the ECPA and Section 2709.

1. Macro-Level Analysis

In 1986, when the ECPA was drafted, the first SNS had yet to be created.[37] Logically, the non-existence of a SNS necessitates the conclusion that Apps were similarly non-existent in 1986. In fact, it was not until 1997, 11 years after enactment of the ECPA, that the first SNS, SixDegrees, was

Cray2_Brochure001.pdf.

[35] *See generally* 18 U.S.C. § 2709 (2015).

[36] TATA CONSULTANCY SERVS., *supra* note 17.

[37] *See generally id.* at 5.

produced.[38] The first of its kind, SixDegrees offered relatively simple functions, allowing its users to maintain a profile, invite friends, search other user profiles, and send instant messages among friends.[39] However, SixDegrees quickly became obsolete and shut down just four years later.[40] Nonetheless, in the following years, the concept of a SNS blossomed and the influx of new and innovative SNSs proved incessant.[41]

By 2007, just 10 years after SixDegrees was created, the number of SNSs had grown considerably, including some of the major forces in the modern SNS arena such as Facebook, YouTube, Reddit, Twitter, and Tumblr.[42] Since 2007, the entrance of innovative and popular SNSs into the market has only accelerated, as established by the emergence of household SNS names such as WhatsApp, Instagram, Snapchat, Tinder, and Bumble.[43] While the aforementioned list comprises a collection of perhaps the most popular SNSs, they represent just a fraction of the number of available SNSs.[44]

In 2017, 20 years after the creation of the first SNS, hundreds of SNSs collectively offer thousands of Apps.[45] In contrast to the approximately one million global users on SixDegrees, the number of people across the globe currently using a SNS stands in excess of two billion.[46] And while the total

---

[38] *The History of Social Networking*, DIG. TRENDS (May 12, 2016, 2:41 PM), http://www.digitaltrends.com/features/the-history-of-social-networking [hereinafter DIG. TRENDS].
[39] *Id.*
[40] *Id.*
[41] *See generally id.*
[42] Kathy Colaiacovo, *An Interesting Timeline of the Evolution of Social Media*, PEPPER IT MARKETING (Jun. 20, 2015), http://www.pepperitmarketing.com/facebook/evolution-social-media.
[43] *Id.*
[44] *See generally* Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, 4285 LECTURE NOTES IN COMP. SCI. 36 (2006).
[45] *Id.*
[46] *Social Media Statistics*, STATISTA, https://www.statista.com/topics/1164/social-networks (last visited Jan. 2, 2016).

number of SNS users in 1997 was roughly one million, currently 78 percent of the adult population in the United States has a SNS profile, totaling approximately 190 million users.[47] In other words, since SixDegrees was created 20 years ago, the number of adults in the United States using a SNS has increased by an average of 9.5 million annually.[48] Although drastic, the increase in the number of SNSs, the number of Apps available, and the number of Apps used has remained consistent. Much like Moore's Law, this trend provides little reason, if any, to doubt more of the same in the years to come.[49]

2. Micro-Level Analysis

Essentially, an App is a ready-made software program provided by a SNS allowing individuals to channel their services remotely.[50] Accordingly, Facebook, in its capacity as a SNS and as owner of Facebook, Instagram, and WhatsApp, provides a number of related Apps to allow users to do just that.[51] In doing so, Facebook provides millions of citizens with the opportunity to conduct mobile, on-the-go transmissions of both content and non-content information through the average smartphone.[52]

Varying from the Facebook App to the Instagram App to the WhatsApp App and so on, communications conducted through Apps range broadly in both form and substance, providing individuals with the ability to transmit virtually any form of information conceivable.[53] In contrast to SixDegrees,

---

[47] *Id.*
[48] *Id.*
[49] *See generally* TATA CONSULTANCY SERVS., *supra* note 17.
[50] John G. Locallo, *'Appy 'Olidays! Deck Your Smartphone and Tablet with Some of These Lawyer-Friendly Apps*, 99 ILL. B.J. 602, 602 (2011).
[51] McGarry, *supra* note 1.
[52] *See generally Most Famous Social Network Sites Worldwide as of September 2016, Ranked by Numbers of Active Users (in Millions)*, STATISTA, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users (last visited July 7, 2017).
[53] *See generally* Julie Ingle, *Evolution of Enterprise Mobile Messaging*, MAGNET (Aug. 21, 2015), https://www.magnet.com/blog/evolution-of-enterprise-mobile-messaging.

which offered the relatively simple functions of profile maintenance, adding friends, and instant messaging, the functions of modern Apps reflect a new era of communication.[54]

Widely regarded as the gold standard among current SNSs, Facebook was invented in 2004.[55] In contrast to its one million monthly users in 2004, by 2016 the number of monthly users on Facebook multiplied approximately 1,700 times, and is currently listed at 1.71 billion users.[56] Specifically within the United States, 79 percent of internet users maintain a Facebook profile.[57] Aside from the increase in Facebook users, perhaps the most remarkable advancement within Facebook has been the development in the technology of its Apps.

While Facebook was not accessible on any mobile device in 2004, Facebook is now available on every smartphone, providing a number of Facebook-specific Apps with unique purposes.[58] The two most popular are the Facebook App and the Facebook Messenger App.[59] Although similar in name, these two Apps provide distinct communicational features.[60] The Facebook App allows users to access most of Facebook's main features from their phone, namely profile management, adding friends, liking comments, watching and posting videos and pictures, and posting on other users' profiles.[61] While much can be

---

[54] *See generally id.*
[55] Susan Dumont, *Campus Safety v. Freedom of Speech: An Evaluation of University Responses to Problematic Speech on Anonymous Social Media*, 11 J. BUS. & TECH.
L. 239, 240 (2016).
[56] *Statistics and facts about social media usage*, STATISTA,
https://www.statista.com/
topics/1164/social-networks (last visited Jan. 2, 2017).
[57] *Percentage of U.S. internet users who use selected social networks as of April 2016*, STATISTA, https://www.statista.com/statistics/246230/share-of-us-internet-users-who-use-selected-social-networks (last visited Jan. 2, 2017).
[58] Taylor Casti, *The Evolution of Facebook Mobile*, MASHABLE (Aug. 1, 2013),
http://mashable.com/2013/08/01/facebook-mobile-evolution/#yqgokdsZp8q4.
[59] *See generally id.*
[60] *Id.*
[61] *Facebook*, iTUNES PREVIEW (Jul. 6, 2017), https://itunes.apple.com/us/app/facebook/id284882215?mt=8.

communicated through this App, most of these features are straightforward and, with the exception of the heightened multimedia capacities, do not deviate significantly from the technological capacities of even the earliest SNS Apps.[62]

However, the Facebook Messenger App provides features that truly encapsulate the technological evolution central to the thesis of this Comment. The Facebook Messenger App provides its users with the opportunities to communicate and engage using everything from relatively simple messaging features to the most technologically advanced processes that the digital age has to offer.[63] For instance, through the Facebook Messenger App, users may send individual and group instant messages, both domestically and internationally, conduct both phone calls and video calls through the internet, share geographical location through GPS technology, send voice messages in text message form, send touchpad created drawings and writings, and even send money through linked bank accounts.[64] Each of these messages arrives with its own distinct notification format.[65] In other words, receipt of an instant message takes a different form than receipt of a money payment, or a GPS location share.[66]

Accordingly, with Apps such as Facebook Messenger, concepts behind electronic communications such as a "message" now hold a more nuanced meaning.[67] Because a "message" sent through Facebook Messenger is not necessarily a typed textual message, it does not necessarily arrive in a manner similar to that of the contents of a letter within a physical envelope.[68] Nevertheless, the FBI may require any SNS to disclose the non-content information of a message sent through Facebook Messenger, and similar Apps, as though such messages were in

---

[62] *See generally id;* DIG. TRENDS , *supra* note 38.
[63] *Conversations Come to Life on Messenger*, MESSENGER, https://www.messenger.com/features (last visited Jan 1, 2017) [hereinafter MESSENGER].
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*

fact analogous to the contents of a physical letter.[69] The FBI is authorized to do so by statutes that were crafted before SNSs and Apps existed, while the internet itself was still in its relatively early stages of development.[70] Brief consideration of the purposes and requirements of these statutes illustrates just how much technology has developmentally outpaced the laws that govern it.

II. OVERVIEW OF STATUTORY AUTHORITY ON NSLS

The four legislative acts that authorize the government to issue NSLs as administrative subpoenas are the Fair Credit Reporting Act ("FCRA"), the National Security Act ("NSACT"), the Right to Financial Privacy Act ("RFPA"), and the Electronic Communications Privacy Act ("ECPA").[71] Along with these four acts, subsequent legislation, such as the USA PATRIOT Act ("PATRIOT Act"), has contributed a great deal to broadening the government's authority to issue NSLs.[72] Each of these acts allows the FBI to obtain distinct categories of information through the issuance of NSLs.[73] Consider each of the following:

A. The FCRA

Enacted in 1970 and codified at 15 U.S.C. § 1681(u)-(v), the aim of the FCRA, is to guarantee citizens the protection of their personal information collected by credit reporting agencies.[74] Nonetheless, the FCRA carves out an exception permitting the FBI to issue a NSL to obtain a consumer reporting agency's credit reports and "all other" consumer information in its files.[75] The FBI can access the full credit reports of citizens

[69] 18 U.S.C. § 2709 (2015).
[70] *See generally* 18 U.S.C. § 2709 (2015); RICHARD M. THOMPSON & JARED P. COLE, CONG. RES. SERV., R44036, STORE COMMUNICATIONS ACT: REFORM OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) (2015).
[71] U.S. DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS 11 (2007), https://oig.justice.gov/reports/2016/o1601b.pdf
[72] *Id.* at 16.
[73] *Id.* at 11.
[74] *Id.* at 13.
[75] *Id.*

through such a NSL as long as the Director of the FBI, or his designee, determines that the information is "sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities."[76] NSLs issued pursuant to the FCRA contain an attendant gag order prohibiting credit-reporting agencies from disclosing that the FBI has sought or obtained records from their agency.[77]

B. The RFPA

Enacted in 1978, the dual objectives of the RFPA, codified at 12 U.S.C. § 3414, are to prevent intrusion into the protected financial records of citizens while still permitting legitimate law enforcement activity.[78] The RFPA allows the FBI to issue NSLs for investigations involving counterintelligence.[79] These NSLs require that financial institutions and their employees comply with FBI requests as long as the FBI has certified that the records are sought for counter-intelligence purposes to protect against international terrorism or clandestine intelligence activities.[80] Similar to the FCRA, NSL's issued pursuant to the RFPA contain a gag order prohibiting recipients from disclosing that the FBI has sought or obtained records from their agency.[81]

---

[76] 15 U.S.C. § 1681u (a)-(b) (2015). Disclosures to FBI for Counterintelligence purposes:

> (b) . . . A consumer reporting agency shall furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request that includes a term that specifically identifies a consumer or account to be used as the basis for the production of that information, signed by the Director or the Director's designee . . . which certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

[77] *Id.*

[78] U.S. DEP'T OF JUSTICE, *supra* note 71.

[79] *Id.* at 12.

[80] 12 U.S.C. § 3414(a)(5)(A) (2015).

[81] 12 U.S.C. § 3414(c)(1)(A)-(B) (2015).

C. The NSACT

The NSACT, codified at 50 U.S.C. § 3162, was amended in 1994 to provide NSL authority.[82] The NSACT allows the FBI to issue NSLs requesting citizens' financial records or consumer reports from financial agencies, financial institutions, holding companies, or any consumer reporting agencies.[83] As a procedural matter, the NSACT allows the issuance of NSLs only where the records sought pertain to a person who is a current or former employee of the executive branch.[84] The NSACT also requires either (1) that the FBI demonstrate reasonable grounds to believe, based on credible information, that the former employee is, or may be, disclosing classified information in an unauthorized manner to a foreign power or the agent of a foreign power; (2) that the information upon which the government relies indicates that the former employee has incurred excessive debt or has acquired a level of affluence that cannot otherwise be explained; or (3) that the circumstances indicate that the former employee had the capability and opportunity to disclose classified information which is now known to have been lost or compromised to a foreign power or the agent of a foreign power.[85] NSLs issued pursuant to the NSACT contain an attendant gag order identical to the gag order stipulated in both the FCRA and RFPA.[86]

D. The ECPA

The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act ("SCA") are jointly referred to as the Electronic Communications Privacy Act of 1986 ("ECPA")[87] and codified at 18 U.S.C. § 2709.[88] The ECPA

---

[82] 50 U.S.C. § 3162(a)(1) (2015).
[83] *Id.*
[84] 50 U.S.C. § 3162(a)(2)(A) (2015).
[85] 50 U.S.C. § 3162(a)(2)(B)(i)-(iii) (2015).
[86] 50 U.S.C. § 3162(b)(1)(A)-(B) (2015).
[87] *Electronic Communications Privacy Act of 1986 (ECPA)*, U.S. DEP'T OF JUSTICE: JUSTICE INFORMATION SHARING (Jul. 30, 2013), https://it.ojp.gov/privacyliberty/authorities/statutes/1285 [hereinafter U.S. DEP'T OF JUSTICE: JUSTICE INFORMATION SHARING].

was crafted to protect the electronic, oral, and wire communications of United States citizens.[89] Unlike the financial subject matter of the previous three acts, however, the ECPA broadly covers transactional information contained within email communications, telephone communications, and other electronically stored communications.[90] Distinct in its focus, the ECPA alone provides a window into general communications and messages between citizens.[91]

The ECPA is comprised of three Titles:[92] Title I covers the use of wiretaps to intercept wire, oral, and electronic communications;[93] Title II covers the SCA and the protection of privacy interests in content and non-content transactional information;[94] and Title III covers the use of pen register or trap and trace devices.[95] Because of its applicability to the substance, at any level of content, of messages sent through SNS Apps, this Comment narrows its focus to Title II, specifically addressing the statutory provisions of Section 2709.[96]

Generally, the purpose of Title II is to uphold the protections of citizens against unlawful intrusion into their electronic and wire communications.[97] However, for the purposes of national security, Section 2709 carves out an exception allowing the FBI access to non-content information upon a relatively modest showing that the information sought is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities."[98] Thus, while Section 2709 has provided citizens with a layer of protection against intrusion into their electronic and wire

---

[88] CHARLES DOYLE, CONG. RES. SERV., R41733, PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 6 (2012).
[89] U.S. DEP'T OF JUSTICE: JUSTICE INFORMATION SHARING, *supra* note 87.
[90] *Id.*
[91] *Id.*
[92] *See generally* 18 U.S.C. §§ 2510-22 (2015).
[93] *See generally* 18 U.S.C. §§ 2701-12 (2015).
[94] *See generally* 18 U.S.C. §§ 2701-12 (2015).
[95] *See generally* 18 U.S.C. §§ 3121-27 (2015).
[96] 18 U.S.C. § 2709.
[97] U.S. DEP'T OF JUSTICE, *supra* note 71, at 12.
[98] 18 U.S.C. § 2709(b)(1) (2015).

communications, it has simultaneously cracked open the door to a disconcertingly wide exception to those exact protections.[99]

Accordingly, pursuant to this exception, the FBI has routinely sought to compel the disclosure of such information through the issuance of NSLs upon SNSs regarding messages sent through their Apps.[100] As with the FCRA, the RFPA, and the NSACT, a NSL issued under the ECPA carries with it an attendant gag order, forbidding disclosure that the FBI has sought or obtained relevant records.[101]

III. THE TROUBLESOME FOURTH AMENDMENT IMPLICATIONS WITHIN THE ECPA

The vital inquiry, for the purposes of this Comment, is whether the process of divulging non-content information subject to disclosure under the ECPA and Section 2709 reveals Fourth Amendment protected communications of SNS App users to the FBI.[102] To resolve this inquiry in the affirmative, it must be the case that either (a) the non-content information is itself somehow protected by the Fourth Amendment, or (b) separation of the non-content information from the content information is impossible. The former requires application of the reasonable expectation of privacy test as outlined in *Katz v. United States*, while the latter involves a more practical inquiry into the technological nuances of the digital age. The remainder of this Section is thus split between these two inquires.

A. Fourth Amendment Protection of Non-Content Information Itself

In *Katz v. United States*, Justice John Marshall Harlan II introduced a test that established reasonable expectations of privacy as constitutionally protected through the Fourth

[99] 18 U.S.C. § 2709(b)(1)-(2) (2015).
[100] *National Security Letter (NSL) FAQ*, ELEC. FRONTIER FOUND., https://w2.eff.org/Privacy/nslfaq.php (last visited Oct. 14, 2016).
[101] 18 U.S.C. § 2709(c)(1)(A)-(B) (2015).
[102] *See generally* 18 U.S.C. § 2709 (2015).

Amendment.[103] The *Katz* test asks first whether an individual expressed a subjective expectation of privacy, and second whether that expectation is one that society would deem objectively reasonable.[104] With this test, the Supreme Court introduced the novel concept that physical trespass is not necessary to find that a Fourth Amendment violation has occurred.[105] This precedent paved the way for Fourth Amendment applications that could adapt to ever-changing societal circumstances.[106]

Thus, despite the speedy evolution of SNS App technology and the incessant development of the communications transmitted therewith, the *Katz* test provides a straightforward process by which the constitutionality of a NSL can be determined and re-determined at any time. In other words, because the *Katz* test acknowledges ongoing changes in technology, it can be used to determine whether, considering the changes in SNS App technology within the context of the digital age, a NSL seeking the non-content information of messages sent through an App violates the Fourth Amendment.

The technology through which the non-content information of modern messages is sent and received has developed greatly since the drafting of the ECPA in 1986, when electronic communications were still in a stage of relative infancy. At that time, the non-content information of an electronic communication referred, by default, only to the parties to, time stamps of, and subject headers of, email correspondences.[107] Three decades later, however, emailing is just one of countless forms of electronic communication.[108] Put plainly, electronic communication through SNS Apps is far more complex and technologically advanced than the emails of the mid-eighties.[109] Accordingly, that which qualifies as non-content

---

[103] Katz v. United States, 389 U.S. 347, 361 (1967).
[104] *Id.*
[105] *Id.*
[106] *See generally id.*
[107] *See generally* NAT'L ASS'N OF CRIM. DEF. LAW., *supra* note 8, at 4-6.
[108] *See generally* Wilson, *supra* note 7, at 5-7.
[109] *See generally id.*

information has undergone a process of development as well.[110] At present, there exist instances in which an individual may hold a reasonable expectation of privacy in the non-content information of her App messages, or at least a viable argument regarding such expectation.

The very nature of certain messages that can now be sent through Apps requires a thorough reconsideration of what qualifies as non-content information and, consequently, is not adequately protected by the Fourth Amendment.[111] As aforementioned, through modern SNS Apps, individuals can transmit more than ever before, including their GPS location, money, recorded video or photo messages, self-made artwork, and so on.[112] Consider, for example, the Facebook Messenger App, in which the communicational features offered are far more complex than even that of modern emailing.[113] The non-content information of a GPS location-sharing message or money payment message through Facebook Messenger may reveal significantly more than the mere list of parties, subject header, and time stamps of an email correspondence. While this Comment does not argue that an individual holds an outright privacy expectation deemed objectively reasonable by society in the non-content of an email correspondence, this Comment does not concede that holding a reasonable expectation of privacy in some other form of non-content information is, by default, implausible.

Consider a hypothetical instance in which the FBI issues a NSL to Facebook seeking the non-content information contained in a GPS location-sharing message sent through Facebook Messenger. If Facebook complies with this NSL, it may turn over to the FBI not only the identities of the parties sharing location, but also transactional records including the times at which the parties shared location, the length of time during which the parties shared location, the IP addresses of each party, and the subject line of the location-sharing message, all of which

110 *See* NAT'L ASS'N OF CRIM. DEF. LAW., *supra* note 8.
111 *Id.*
112 *Id.*
113 *See generally* MESSENGER, *supra* note 63.

might reveal even more about where the user is or the user's reasons for being there. In another hypothetical scenario, the FBI might issue a NSL to Facebook seeking the non-content information contained in a money payment message sent through Facebook Messenger. If Facebook complies with this NSL, it may turn over to the FBI not only the identities of the parties involved in the money transaction, but the transactional records including the time of payment, the amount paid, and the subject line of the payment message, which may include, as it often does, the reason the payment was exchanged. Such NSLs, although authorized by the ECPA and presently lawful, may give rise to a viable complaint of Fourth Amendment violation.

Despite the increasingly revealing nature of non-content information, even were it presumed that non-content information cannot itself be protected by the Fourth Amendment, the inquiry remains as to whether non-content information can be separated from content information in all instances.

B. Inseparability of Non-Content Information and Content Information

In discussing the inseparability of non-content information and content information, it is helpful to consider the difference between hard-copy communications, such as physical letters, and electronic communications, such as SNS App messages. If the government sought to review only the non-content information contained in a physical letter, the process of limiting its review would be relatively straightforward, as the government would need only to abstain from opening the envelope.[114] The envelope of a physical letter, sent through the postal service, cannot reveal anything more than the identity of the sender, the identity of the recipient, each party's respective mailing address, and the date of the mailing. By contrast, the distinction between content and non-content information in the context of electronic communications can be far more

[114] *See generally* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2112 (2009).

complicated.[115] Non-content information, or the analogous "envelope," of a message sent through a SNS App is not necessarily a mere container of a message. There are now thousands of SNS Apps available to citizens, and hundreds of thousands of different ways to send a message.[116] Modern SNS App messages are not limited to a basic formula of content-inside-envelope.[117] In fact, with the features of certain SNS Apps, some or all of the substance of a message itself may be revealed within the non-content information, or envelope itself.[118]

In addition to the crucial distinctions between the process of sending an electronic communication and the process of sending a hard copy communication, there are also important distinctions between the various processes of electronic communications.[119] In other words, not all electronic communications are built the same. For instance, the process of sending a message through Facebook Messenger can involve a far more complicated technological process than that of sending a basic email.[120] The transmission of such instant and hybridized messages through Facebook Messenger and other similar Apps is distinct in several important ways from the careful and premeditated process of crafting an email, which was contemplated by the drafters of the ECPA.[121]

First, in contrast to the process of basic emailing, communications transmitted through modern SNS Apps are sent in volumes unanticipated by the original drafters of the ECPA and Section 2709.[122] Whereas even premier email providers place daily limits on the number of emails that can be sent from

---

115 *See* NAT'L ASS'N OF CRIM. DEF. LAW., *supra* note 8.
116 DIG. TRENDS , *supra* note 38.
117 *See generally* TATA CONSULTANCY SERVS., *supra* note 17.
118 *See generally* NAT'L ASS'N OF CRIM. DEF. LAW., *supra* note 8, at 5-6.
119 Brian Jung, *Six Types of Electronic Communication*, TECHWALLA, https://www.techwalla.com/articles/six-types-of-electronic-communication (last visited Jul. 7, 2017).
120 *See generally* MESSENGER, *supra* note 63.
121 *See* Frederick M. Joyce & Andrew E. Bigart, *Liability for All Privacy for None: The Conundrum of Protecting Privacy Rights in a Pervasively Electronic World*, 41 VAL. U.L. REV. 1481, 1487 (2007).
122 *Id.*

one account, or the amount of recipients per each message, SNS Apps contain no limits on the quantity of messages, number of recipients, or anything, for that matter.[123] Thus, both the number of electronic messages sent through SNS Apps as well as the number of individuals involved in such messages may greatly exceed that of email providers.

Second, the technological complexity of messages sent through SNS Apps is far more advanced than that of the basic emailing envisioned by the drafters of the ECPA.[124] The basic functions of emailing are relatively rudimentary, typically involving a header, subject, date, attachments, and list of senders.[125] By contrast, in addition to such basic features, modern SNS Apps provide myriad advanced features including, but not limited to, multimedia messaging options, video and photo interface options, artwork sharing, URL link sharing, collaborative gameplay, location sharing, financial transactions, and instant messaging features.[126]

Further, whereas the substance of an email message is found exclusively within the body of that email, the substance or content of a SNS App message may at times be enmeshed with the notification or envelope of the message.[127] Put more descriptively, while an email recipient must follow a multi-step process and affirmatively select options in order to proceed past the notification onto the actual body of a message or the actual content of an attachment, recipients of a SNS App message may be able to deduce some, if not all, of the message without ever proceeding past the analogous envelope.[128]

---

123 *See Gmail Sending Limits in G Suite*, GOOGLE, https://support.google.com/a/answer/166852?hl=en (last visited Dec. 15, 2016); Steve Kovach, *The 8 Best Apps for Free Texting*, BUS. INSIDER (Jan. 29, 2011, 5:04 PM), http://www.businessinsider.com/apps-you-can-ditch-your-text-message-plan-for-2010-11.

124 *See* Adam I. Cohen & David J. Lender, *Email and Collaboration Systems: Standard Email Systems*, ELECT. DISC. L. & PRACT. § 20.01 (2016).

125 *Id.*

126 Wilson, *supra* note 7, at 7.

127 *See* NAT'L ASS'N OF CRIM. DEF. LAW., *supra* note 8.

128 *See generally* Cohen & Lender, *supra* note 1.

For example, consider a hypothetical instance in which the FBI issues a NSL that provides access to a message sent through Facebook Messenger involving a URL link within the header or subject line.[129] That URL link might include the search query followed by the sender of the message.[130] So, one such NSL may divulge to the FBI the words searched by the sender of the message, granting insight into the substance or purpose of that communication, and the government need go no further than the non-content information of the message to retrieve as much.[131]

Another scenario demonstrating the inseparability of non-content and content information arises within the context of group messages that can be transmitted on any number of SNS Apps, from WhatsApp, to Facebook Messenger, to GroupMe, and so on.[132] Consider that, in many group messaging Apps, any member of the group chat can alter the title or name of the group chat, add or subtract members within a group chat, or even edit the photograph that appears as the default image of the group chat.[133] So, while the name of a group chat may not be considered the intended forum for discourse between members to the group, the fact of the matter is that with modern technology, App users can depart from conventional boundaries and defy outdated norms and limitations of message sending.[134] Accordingly, the substance of electronic communications can fathomably be discovered from the subject line or the title of a group chat, which traditionally contained just name of the parties involved.[135]

---

[129] NAT'L ASS'N OF CRIM. DEF. LAW., *supra* note 8.
[130] *See id.*
[131] *Id.*
[132] *See generally* Jon Russell, *22 of the Best Mobile Messaging Apps*, TNW (Aug. 1, 2014), http://thenextweb.com/apps/2013/10/18/best-mobile-messaging-apps.
[133] *See generally* David Nield, *The Best Group Messaging Apps*, GIZMODO (Nov. 7, 2016, 8:39 AM), http://fieldguide.gizmodo.com/the-best-group-messaging-apps-1788648894.
[134] *See generally id.*
[135] *See id.*

As these examples demonstrate, content information can now be divulged where only non-content information is intended. The barrier between these two categories of information is evaporating with the influx of complex modern App technologies. Thus, the relevant statutes, which impose different standards of FBI access based on the difference between non-content and content information, must be amended so as to accommodate and respond to the evolution of their subject matter. The following proposed amendments to the ECPA allow for just that.

IV. RECOMMENDATIONS

The process of rectifying the inadequacies of Section 2709 is multifaceted: (A) the language of several subsections should be amended to provide citizens with the assurance that, if the government seeks their non-content information through a NSL, it will only be able to do so in compliance with the protections of the Fourth Amendment against unreasonable searches and seizures; and (B) Congress should make a firm commitment to legislative adaptability in regards to re-evaluating Section 2709, and the ECPA as a whole, as technology evolves to ensure that our legislation is not outdated and permissive of Fourth Amendment violations.

A. Amending the Language of Section 2709

1. Inclusion of Definition Subsection

First and foremost, Section 2709 should be amended to include a "Subsection h" providing definitions for several terms that, although currently used throughout the Section, are not sufficiently defined. While the phrase "subscriber information and toll billing records information, or electronic transactional records" has been understood to collectively refer to non-content information, this connotation is not provided within the text of

the statute.[136] Adding "Subsection h" would remedy this uncertainty by plainly defining non-content information.

Proposed "Subsection h" reads in the following manner:

(h) Definitions – For the purposes of this Section, the term "non-content information" means any of the following:
(1) Subscriber Information, including:
(a) The full names of the parties to the communication; or
(b) The email address under which each party is a subscribed member of the wire or electronic communication service provider; or
(c) The phone number under which each party is a subscribed member of the wire or electronic communication service provider; and
(2) Toll Billing Records Information, including:
(a) The phone number used by the caller;
(b) The numbers dialed by the caller; or
(c) The time duration of the call.
(3) Any information not explicitly listed within Subsections (1)-(2) does not qualify as "non-content information."

This amendment is beneficial in two crucial ways. First, this amendment removes any reference to "electronic communication transactional records," which served only to broaden the FBI's NSL power past ordinary telephone services.[137] This amendment retains that broadening effect by including "the email address under which each party is a subscribed member of the wire or electronic communication service provider" as part of the definition of subscriber information. However, unlike the original language of Section 2709, this amendment removes any ambiguity as to whether the term "electronic communication transactional records"

[136] 18 U.S.C. § 2709(a) (2015).
[137] Requests for Information Under the Electronic Communications Privacy Act, 32 OP. O.L.C. 145, 147 (2008).

broadened the meaning of non-content information with regards to the substance of the transaction. Second, this amended definition section introduces clarity into Section 2709 by dispelling any ambiguity as to which information qualifies as non-content information and is, thus, amenable to a NSL and unprotected by the Fourth Amendment.

2. Amending the Language of Section 2709(b)(1)-(2)

The current Section 2709(b)(1)-(2) describes the information obtainable by the FBI, along with the FBI's burden to obtain that information.[138] However, in light of this Comment's proposed amendment to "non-content information," which tightens the definition of obtainable information under Section 2709(a), the immediate amendments serve only to amend obtainable information in a consistent fashion. This Comment's first proposed amendment, if enacted, alleviates any need to heighten the burden on the FBI.

Starting at the beginning of Section 2709(b)(1), this Comment proposes to amend the statute to provide that the FBI may:

> request non-content information of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the non-content information sought is relevant to an authorized investigation against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment of the Constitution of the United States.

The relevant portions of Section 2709(b)(2) shall be amended in the same manner.

These proposed amendments address the concern that certain elements of an electronic communication, which have

[138] 18 U.S.C. § 2709(b)(1)-(2) (2015).

been referred to broadly as non-content information, may in fact reveal content or the substance of a message. The above amendments duly acknowledge the evolution of such electronic communications, such as messages through SNS Apps, by restricting the definition of non-content information to the elements of these messages which cannot reveal any part of the substance of a communication. This prescriptive amendment solves the legal problem which arose from the simultaneous evolution of what was once considered non-content information and the stagnation of statutory authority governing FBI access to such information.

3. Additional Prohibition Regarding the Disclosure of Non-Content Information

The final amendment adds a new subsection to Section 2709. The newly created "Subsection i" addresses the instances in which the non-content information sought is inseparable from the content information, as discussed in Part III, Subsection B of this Comment. "Subsection i" remedies this complication by plainly prohibiting access to such non-content information. Proposed "Subsection i" reads in the following manner:

> (i) Prohibition of Certain Disclosure. – If a request is made by the FBI, it cannot be executed where the wire or electronic communication service provider is unable to separate the otherwise lawfully obtainable non-content information from information that is not lawfully obtainable.

This final amendment to Section 2709 acknowledges the complexity of certain electronic communicational technologies. Because certain SNS Apps allow users to communicate in a manner in which the substance of their communication may be divulged within what has traditionally been considered the non-content of a communication, this amendment takes appropriate heed by prohibiting the disclosure of any such non-content information. In doing so, this amendment protects citizens' Fourth Amendment rights in the instance where the government seeks non-content information, but technological impossibility

binds disclosure of such non-content information with the disclosure of Fourth Amendment protected communications.

B. Congressional Commitment to Legislative Adaptability

Secondly, the long-term solution to ensuring adequate protection of the Fourth Amendment rights of citizens is an ongoing effort by Congress to amend Section 2709 to ensure it is up to speed with its subject matter. This may require, for example, a regular consultation with a newly created Congressional committee that specializes in technological advances of electronic communication technologies.

The exact form that future legislative adaptability will take is a determination for another date. Nevertheless, the need for such ongoing statutory adjustment is ultimately more vital than the provision of immediate amendments to the current legislation. Acknowledging that it is impossible to develop one static set of laws that can anticipate and accommodate the permutations of computer and SNS App technology, as well as the novel strands of non-content information that attend such technological advancement, the long-term resolution to the legal problem at hand cannot simply be a singular set of amended laws.

V. CONCLUSION

Due to the drastic development of computer technology following the passage of the ECPA, individuals can now store powerful computers, in the form of smartphones, conveniently inside of their pockets.[139] The simultaneous evolution of SNS and App technology allows these individuals to use such computers to send and receive endless volumes and types of information instantly.[140] In 1986, the drafters of the ECPA could not possibly have contemplated the statute's applicability to the subsequently

[139] *See generally* APPLE, *supra* note 28.
[140] *See generally* MESSENGER, *supra* note 63.

invented SNSs or Apps.[141] Nevertheless, the ECPA has been consistently applied as the governing authority on FBI NSLs issued upon SNSs regarding messages transmitted through their Apps.[142] The problem remains, however, that by virtue of its antiquity, the ECPA is ill equipped to apply to SNSs and related Apps while still heeding the inherent privacy interests at play with such technologies.

The ECPA, specifically the text of Section 2709, currently arms the FBI with an investigative scope so imprudently broad as to confer upon it the power to issue NSLs that circumvent the reasonable expectation of privacy test, as outlined in *Katz v. United States*.[143] Accordingly, to ensure that continued government issuance of NSLs does not run afoul of the Fourth Amendment, Congress must amend Section 2709 to acknowledge the evolution of electronic communications technologies that has reshaped the concept of non-content information. Additionally, Congress must provide an ongoing commitment to legislative adaptability in order to preserve the efficacy of Section 2709 and other NSL-authorizing statutes, and to keep such statutes on pace with their subject matter.

Regardless of the approach that Congress takes to demonstrate legislative adaptability, the crucial point is that Congress must manifest a willingness to revise and acclimate the relevant statutory authority to technological evolutions. Thus, a sustainable legal solution is a continued effort by Congress to provide its constituents with adequate protection from unreasonable searches and seizures in violation of the Fourth Amendment, even where developments of the digital age require a reconsideration of the electronic landscape on which we communicate.

[141] Alex Brown, *Derivative-Consent Doctrine and Open Windows: A New Method to Consider the Fourth Amendment Implications of Mass Surveillance Technology*, 66 CASE W. RES. L. REV. 261, 263 (2015).
[142] U.S. DEP'T OF JUSTICE, *supra* note 71, at 12-13.
[143] Katz v. United States, 389 U.S. 347, 360 (1967).