5-1-2014

Where's Waldo? Who's Asking?!!? A Better Way to Think About Location Data Privacy

Mark A. Basanta

WHERE'S WALDO? WHO'S ASKING?!!? A BETTER WAY TO THINK ABOUT LOCATION DATA PRIVACY

*By: Mark Basanta**

Introduction

The information age has wrought technology inconceivable to people of any prior age in human history. As the name suggests, this age is "marked by the increased production, transmission, consumption of and reliance on information."[1] True to form, Americans are prolific data producers.[2] We generate approximately 2.5 quintillion bytes of data every day.[3] Roughly speaking, this is more than 13 trillion books or 90 million Blu-Ray discs worth of data *every day*.[4] Rightly or wrongly, we expect our data to be private.[5] Unfortunately, that expectation is under assault from two overwhelming forces. Against the market forces of commerce[6] and the coercive power of the state, "[t]he right of the people to be secure in their . . . papers, and effects"[7] is more threatened now than at any time since 1789. However, the nature of the Fourth Amendment and the current state of its jurisprudence means that we cannot rely on it for personal privacy in this age.[8] Therefore, legislators must fill the weighty role of privacy protectors to the American people. But try as they have, current federal legislation protecting the data of American citizens is ambiguous and not consistently applied. A recent pair of high-

---

* Juris Doctor Candidate, anticipated 2014, Seton Hall University School of Law; Bachelor of Engineering in Mechanical Engineering, Stevens Institute of Technology, 1999.

[1] *Glossary of Terms*, HARVARD UNIV., http://cyber.law.harvard.edu/readinessguide/glossary.html (last visited Feb. 3, 2012) (definition of "information age").

[2] *What Is Big Data?*, IBM, http://www.ibm.com/software/data/bigdata/ (last visited Feb. 3, 2013).

[3] *Id.*

[4] *Data Capacity Converter Online*, UNITARIUM.COM, http://www.unitarium.com/data?unit=g1&val=2.5e+18 (last visited Feb. 3, 2013) (one-hundred page books, twenty-five gigabyte Blu-Ray discs).

[5] *See* JENNIFER M. URBAN ET AL., BERKELEY CENTER FOR LAW & TECHNOLOGY, UC-BERKELEY SCHOOL OF LAW, MOBILE PHONES AND PRIVACY 8-9 (2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405

[6] *See* Declan McCullagh, *Verizon Draws Fire For Monitoring App Usage, Browsing Habits*, CNET.COM (Oct. 16, 2012, 5:00 AM), http://news.cnet.com/8301-13578_3-57533001-38.

[7] U.S. CONST. amend. IV.

[8] *See infra* Part I.A.

profile federal cases regarding the privacy of a person's location information has brought this issue to the fore.[9] In *United States v. Jones*,[10] the Supreme Court decided a case in which the government placed a global positioning system ("GPS")[11] device onto a criminal defendant's car in order to track his location.[12] The government did not have a valid warrant.[13] In *United States v. Skinner*, the Sixth Circuit decided a case in which the government tracked a criminal defendant using location data produced by the defendant's cell phone.[14]

The current federal regime[15] relied upon to safeguard personal location data is confusing and uncertain, leading inexorably to the conclusion that it is ill-suited to the purpose. Congress must act on this truth[16] by enacting far-sighted and comprehensive legislation that is technologically agnostic and cognizant of four important dichotomies: (1) The Fact of Location vs. Location Data, (2) Unrevealed Data vs. Revealed Data, (3) Historical Data vs. Prospective Data, and (4) Point-In-Time Surveillance vs. Durational Surveillance. This Note suggests that legislators should use this gaping hole in the law as an opportunity to construct a measure that protects location data privacy immediately and serves as a test case for comprehensive reform of privacy legislation for all forms of personal data in the future. If such a law was wisely and precisely drafted, it would not only stand as a model for data privacy laws in the future but could *become* the data privacy law of the future through careful amendment. The hope is that legislators will be able to flesh out a complete, coherent piece of legislation that protects both

---

[9] United States v. Jones, 132 S. Ct. 945 (2012) and United States v. Skinner, 690 F.3d 772 (6th Cir. 2012), *reh'g and reh'g en banc denied* (Sept., 26, 2012), *petition for cert. filed* (U.S. Dec. 26, 2012).

[10] *Jones*, 132 S. Ct. at 947.

[11] The global positioning system is a network of satellites, run by the United States' military that can be used to determine a person's longitude, latitude, and altitude through the use of a portable device. DANIEL KLEPPNER, NATIONAL ACADEMY OF SCIENCES, THE GLOBAL POSITIONING SYSTEM: THE ROLE OF ATOMIC CLOCKS 1, 7 (Gary Taubes, ed., 1997), *available at* http://www.beyonddiscovery.org/content/view.pdf.asp?a=458.

[12] *Jones*, 132 S. Ct. at 947.

[13] *Id.* at 948 n.1.

[14] *Skinner*, 690 F.3d at 774.

[15] "Current federal regime" refers to the Fourth Amendment and certain federal statutes. *See infra*, Part I.B.

[16] Because of Congress' past activity in this area and Congress' proposals in this same area, it stands to reason that it has significant interest in this area. *See infra* Part I.B.

personal privacy and public interest based on this framework.

In Part I, this Note explores the difficulties inherent in the law currently used to protect user data. Part I then goes on to discuss some general difficulties that legislators and judges have in understanding technology. Part I finishes by showing that judges have concluded there is little they can do to clear up the confusion and the solution must come from the legislature. In Part II, this Note discusses the disparity in the pace of legislative development and technological development, and clarifies the scope of the proposed legislation. Part II concludes by providing examples of technology not covered by current legislation and which remains outside the ambit of typical contemporary legislative proposals. In Part III, this Note discusses the important dichotomies that surface when scrutinizing possible practical and historical bases for a legislative framework, and then discusses other criteria and why they should be discarded. In Part IV, this Note proposes a set of comprehensive definitions for use in the framework and offers a matrix of location data categories, prioritized according to an analysis of the four important dichotomies.

I. Present Protection: Confusing, Uncertain and Ill-Suited

Currently, individuals may defend against a government entity's search or seizure of location data in two principle manners. The first, and arguably the most natural, is by appeal to the Fourth Amendment.[17] The second is by invoking the Electronic Communications Privacy Act ("ECPA").[18] There are fewer options when defending against privacy violations by private entities, such as cell phone service providers. In the private context, a person may only resort to

[17] U.S. CONST. amend. IV.

[18] Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848 (1986). The ECPA is sometimes referred to as the Stored Communications Act. *See, e.g.*, United States v. Graham, 846 F. Supp. 2d 384, 386 (D. Md. 2012); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1033 (2010) [hereinafter *Applying the Fourth Amendment*]. This appears to be a misnomer based on the name given to Chapter 121 of Title 18 of the United States Code: Stored Wire and Electronic Communications and Transactional Records Access. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 n.1 (2004) [hereinafter *A User's Guide*].

the ECPA. Unfortunately, neither the Fourth Amendment nor the ECPA offers much relief.

A. The Fourth Amendment

The Fourth Amendment is generally ill-suited to protect location data against private or government intrusion. The Fourth Amendment offers no protection against intrusion by private actors,[19] and as against government intrusion, the Supreme Court holds that persons travelling in public have no reasonable expectation of privacy in their movements from one place to another because such movements are open to public scrutiny.[20]

United States v. Knotts serves as a useful starting point in examining how the Fourth Amendment is ill suited to protect location data.[21] In *Knotts*, police placed a tracking "beeper" in a five-gallon container of chloroform with consent of the container's then owner.[22] The Court explained that "[a] beeper is a radio transmitter . . . which emits periodic signals that can be picked up by a radio receiver."[23] One of the *Knotts* defendants, an alleged drug manufacturer, subsequently purchased and transported the five-gallon container to another location.[24] The defendant travelled mainly on "public streets and highways" to a second location.[25] The police tracked him "using both visual surveillance and a monitor."[26] The "monitor" "received the signals sent from the beeper."[27] The Court held that the suspect's reasonable expectation of privacy had not been infringed because "the information obtained—the location of the automobile carrying the [beeper] on public roads, and the location of the off-loaded [beeper] in

---

[19] For those unfamiliar with Fourth Amendment jurisprudence, *see generally* 2 Treatise on Const. L. § 16.1(a) (5th ed.).
[20] United States v. Knotts, 460 U.S. 276, 281 (1983).
[21] *Id.* at 276.
[22] *Id.* at 277-78.
[23] *Id.* at 277.
[24] *Id.* at 277-78.
[25] *Id.* at 281.
[26] *Knotts*, 460 U.S. at 278.
[27] *Id.*

open fields near Knotts' cabin—had been voluntarily conveyed to the public."[28] Location data was clearly at issue in *Knotts*, but it is important to note the police owned and operated the tracking device used.[29]

The Sixth Circuit extended the sensible holding of *Knotts*—and indeed relied heavily upon it—to leave unprotected, location data produced by technology owned and operated by an individual.[30] In *Skinner*, police obtained "an order from a federal magistrate judge . . . authorizing the phone company to release subscriber information, cell site information, GPS real-time location, and 'ping' data" for two cell phone numbers.[31] The "order" granted was something less than a search warrant as required by the Fourth Amendment.[32] Skinner, an alleged drug trafficker, was using one of the phone numbers in question.[33] The police used the data obtained through the order to locate Skinner and arrest him.[34] The police did not "conduct any type of visual surveillance."[35] Ultimately, the Sixth Circuit held that the Fourth Amendment was not violated because "Skinner did not have a reasonable expectation of privacy in the data given off by his . . . cell phone."[36] Many lower federal courts agree with this holding,[37] even

---

[28] *Jones*, 132 S. Ct. at 951-52 (citing *Knotts*, 460 U.S. at 281-82).
[29] *See Knotts*, 460 U.S. at 278 ("officers installed a beeper inside a five gallon container").
[30] *Skinner*, 690 F.3d at 777.
[31] *Id.* at 776. Cell site information, GPS location data, and ping data are three different methods of tracking the location of a properly equipped cell phone. Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 126-29 (2012).
[32] *Skinner*, 690 F.3d at 776-77. Skinner challenged the use of the information "emitted from" his cell phone on Fourth Amendment grounds. *Id.* Among the reasons given for rejecting the challenge, a magistrate judge opined that "Skinner did not have a legitimate expectation of privacy in the phone." *Id.* The district court adopted the magistrate judge's opinion. *Id.*
[33] *Id.* at 775.
[34] *Id.* at 776.
[35] *Id.*
[36] *Id.* at 777.
[37] *See, e .g.*, United States v. Suarez-Blanca, CR 1:07CR0023MHS/AJB, 2008 WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008) ("The Court concludes that the government's acquisition of cell site information did not violate the defendant's Fourth Amendment rights."); *Graham*, 846 F. Supp. at 389 ("[T]his Court concludes that the Defendants in this case do not have a legitimate expectation of privacy in the historical cell site location records acquired by the government."); United States v. Madison, 11-60285-CR, 2012 WL 3095357 (S.D. Fla. July 30, 2012) ("[T]he third-party-disclosure doctrine . . . requires the finding that society is not prepared to recognize as legitimate any

while some have held that the Fourth Amendment does protect cell phone location records.[38]

While *Knotts* seems rightly decided, *Skinner* is problematic for two reasons. First, the police in *Skinner* relied heavily upon "ping data,"[39] but the court's holding specifically references data "emanating from"[40] or "given off"[41] by a person's cell phone. "Ping data" does[42] allow police to track a cell phone.[43] However, "ping data" originates with a request from the cell phone provider—in this case, at the request of police—to which the user's cell phone merely responds.[44] In other words, "ping data" is not merely "given off" by a cell phone, it requires active participation by another party. In *Skinner*, the police were not passive data collectors as suggested by the Sixth Circuit.[45] This insight seems to undermine the holding in *Skinner*.[46] The second problem is that future courts could read *Skinner* broadly to include far more than location data. "[D]ata given off by his . . . cell phone" also properly describes voice calls made from cell phones,[47] which seems to suggest that the Sixth Circuit does not extend Fourth Amendment protection to voice conversations had via cell phone.

In light of *Skinner*'s loose analysis, it seems unlikely to maintain its vitality for long.

---

subjective expectation that Defendant might have had in the cell-tower location data for his cell-phone usage.").

[38] *See, e .g.*, In re Application of the United States, 747 F. Supp. 2d 827 (S.D. Tex. 2010); In re Application of the United States, 809 F. Supp. 2d 113, 122 (E.D.N.Y. 2011) ("[T]he court concludes an exception to the third-party-disclosure doctrine should be applied to *cumulative* cell-site-location records.") (emphasis in original).

[39] *Skinner*, 690 F.3d at 776 (relating that police "continuously 'ping[ed]'" Skinner's phone).

[40] *Id.* at 774.

[41] *Id.* at 777.

[42] While some may disagree on the propriety of it, *see* Simon Rogers, *Data Are Or Data Is?*, THE GUARDIAN (July 8, 2012 5:30 AM), http://www.guardian.co.uk/news/datablog/2010/jul/16/data-plural-singular, this Note uses the noun "data" with singular verbs.

[43] Pell, *supra* note 31, at 131-32.

[44] *Id.*

[45] *Skinner*, 690 F.3d at 774 ("The government used data emanating from . . . Skinner's . . . cell phone to determine its real-time location. . . . As a result of tracking the cell phone . . . .").

[46] Michael Hoven, *Sixth Circuit Approves Warrantless Tracking of Cell Phone Location*, HARVARD JOURNAL OF LAW & TECHNOLOGY (Aug. 17, 2012), http://jolt.law.harvard.edu/digest/telecommunications/united-states-v-skinner (collecting commentator opinions to that effect).

[47] Voice calls on modern digital cell phones are merely strings of zeroes and ones as is the data traded between GPS satellites and modern digital cell phones. *See Fact Sheet 2: Wireless Communications: Voice and Data Privacy*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/fs/fs2-wire.htm#introduction (last updated March 2013).

However, its shortcomings—when combined with lower court confusion—highlight the fact that the Fourth Amendment is not presently, and will not soon be, reliable for protecting personal location data against government intrusion.

B. Current Legislation

The federal legislation pressed into service to safeguard personal location data became law in the 1960's and in the 1980's.[48] The three chapters of the U.S. Code implicated are outdated. They are legacies from the days before personal computers or mobile phones became common and before the internet was invented.[49] Congress developed the law in stages, starting in 1968 as a reaction to the seminal Fourth Amendment decision *Katz v. United States*.[50] The Omnibus Crime Control and Safe Streets Act[51] covered numerous, disparate topics.[52] Title III created Chapter 119 in the federal criminal code and relates to wiretapping and electronic surveillance.[53] The next significant step came in 1986 with the passage of the Electronic Communications Privacy Act.[54] This Act extended the protections granted in 1968 to cover new modes of communication, including email.[55] The Act also created the bulk of Chapter 121, which relates to stored communications, and Chapter 206, which relates to pen registers, in the

---

[48] *See* 18 U.S.C. §§ 2510-2513, 2515-2520 (originally enacted in 1968); 18 U.S.C. §§ 2701-2709, 2711, 3121-3124, 3126-3127 (originally enacted in 1986).

[49] *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 701 (2011).

[50] *Jones*, 132 S. Ct. at 963 (Alito, J., concurring). The *Katz* decision introduced Justice Harlan's now famous two-prong test to Fourth Amendment analysis. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

[51] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 197 (1968).

[52] Topics covered include: state firearms control assistance, disqualification for engaging in riots and civil disorder, and confirmation of the director of the FBI. *Id.*

[53] *Id.* at tit. III. Chapter 119 is titled the "Wire and Electronic Communications Interception and Interception of Oral Communications."

[54] Electronic Communications Privacy Act.

[55] Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1564 (2004).

federal criminal code.[56] Together, these three chapters represent the universe of federal legislation protecting user data from government or private intrusion.[57]

The concepts and examples codified by these statutes range from the quaint to the downright incoherent.[58] A prominent incoherency is evident in the statute's conceptual split between an electronic communication service ("ECS")[59] and a remote computing service ("RCS"),[60] and the impact this split has on the privacy of email. At its most simple level, an ECS "provides a service that supports communications by others."[61] An RCS "either store[s] and/or process[es] information on [a] senders' behalf" and "provides a service that supports communications to its systems."[62] An email service provider, like Google with its familiar Gmail service, or Microsoft with its Hotmail service, can fall into either classification.[63] When persons try to invoke the ECPA to protect their email a court must first determine whether the email service provider involved is an ECS or an RCS. The incoherency arises because the level of protection given to the email varies based on this determination.[64] And this determination may turn on something as trivial as whether the email is opened or unopened by the recipient,[65] or whether the email is more or less than 180 days old.[66]

---

[56] Chapter 121 is titled the "Stored Wire and Electronic Communications and Transactional Records Access," and chapter 206 is titled the "Pen Registers and Trap and Trace Devices."

[57] *See* Mulligan, *supra* note 55, at 1565-66.

[58] For example, current law safeguards Americans from "[w]rongful disclosure of video tape rental or sale records." 18 U.S.C. § 2710 (1988). While this section is quaint, it does not mean that a person's video rental history is undeserving of protection *per se*. However, it is notable that the law currently ranks video rental histories in its hierarchy of sensitive personal information while omitting location data entirely.

[59] An electronic communication service is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (2002).

[60] Remote computing service "means the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2) (2009).

[61] Mulligan, *supra* note 55, at 1568.

[62] *Id.*

[63] *Id.*

[64] For a more complete discussion of the difference between ECS's and RCS's, *see Id.* at 1568-71.

[65] *A User's Guide*, *supra* note 18, at 1216.

[66] *See* United States v. Warshak, 631 F.3d 266, 283 (6th Cir. 2010). "The government may obtain the contents of e-mails that are 'in electronic storage' with an [ECS] for 180 days or less 'only pursuant to a warrant.' The government has three options for obtaining communications stored with a [RCS] and communications that have

Furthermore, courts struggle to understand and apply these sections.[67] Both the Fifth and Ninth Circuits have expressed this frustration.[68] From a decision made at the dawn of the internet age, the Fifth Circuit noted that "[u]nderstanding the Act requires understanding and applying its many technical terms as defined by the Act, as well as engaging in painstaking, methodical analysis."[69] Later, the Ninth Circuit observed that the ECPA "is a complex, often convoluted, area of the law," and further noted that the "statutory framework is ill-suited" to the modern age because it was written prior to the advent of the internet.[70] The court then lamented "that until Congress brings the laws in line with modern technology, protection of the Internet and websites . . . will remain a confusing and uncertain area of the law."[71] The same is true of wireless communication services, which did not become prominent until long after Congress' last significant update of the ECPA.

Federal judges at all levels have similarly called for legislative clarity with regard to the protection of location data. Most notable is Justice Alito's concurrence in *Jones*.[72] He first notes that since the Omnibus Crime Control and Safe Streets Act of 1968,[73] statutes—and not the Fourth Amendment—have primarily governed privacy.[74] He goes on to advocate leaving primary responsibility with legislators, opining that a "legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a

---

been in electronic storage with an electronic service provider for more than 180 days: (1) obtain a warrant; (2) use an administrative subpoena; or (3) obtain a court order under § 2703(d)." *Id.* (citations omitted).

[67] Laura J. Tyson, *A Break in the Internet Privacy Chain: How Law Enforcement Connects Content to Non-Content to Discover an Internet User's Identity*, 40 SETON HALL L. REV. 1257, 1284-85 (2010).

[68] *Id.*

[69] Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 461 (5th Cir. 1994) (referring to the ECPA as "the Act").

[70] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (internal quotations omitted).

[71] *Id.*

[72] *Jones*, 132 S. Ct. at 945 (Alito, J., concurring).

[73] Omnibus Crime Control and Safe Streets Act.

[74] *See id.* at 962-63 (Alito, J., concurring); *See also*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004) (suggesting that "statutory rules rather than constitutional rules should provide the primary source of privacy protections regulating law-enforcement use of rapidly developing technologies").

comprehensive way."[75] Lastly, Justice Alito laments that no action has yet been taken by Congress.[76]

Several circuit court decisions suggest that those courts agree. In *United States v. Cuevas-Perez*, the Seventh Circuit noted that the pace of change in location technology "may make the legislature the branch of government that is best suited, and best situated, to act."[77] *Cuevas-Perez* was a case very similar to *Jones*. Without a warrant, police attached a GPS device to a suspected drug distributor's car while it was parked in a public area.[78] The Supreme Court subsequently granted certiorari on *Cuevas-Perez* and handed down its opinion a month after *Jones*.[79] The Court vacated the judgment and remanded for further consideration in light of *Jones*, but the point regarding the legislature being best suited to act remains.[80] In *In re Askin*, the Fourth Circuit urged judicial restraint when faced with new technologies to avoid nullifying "the balance between privacy rights and law enforcement needs struck by Congress" in the ECPA.[81] The court also noted Congress' effort to "legislate comprehensively in this field" and frequent amendments to the ECPA.[82]

The District Courts use similar language. In the *United States v. Graham*, the District Court for the District of Maryland addressed the issue of whether government's obtainment of historical location records from two criminal defendants' mobile telephone service providers violated the Fourth Amendment or the terms of the ECPA.[83] In its discussion, the court noted

---

[75] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).
[76] *Id.* (Alito, J., concurring). In *Jones*, the Court was concerned with the use of government provided "GPS tracking technology for law enforcement purposes," but the same applies to invasions of personal location data. *Id.*
[77] United States v. Cuevas-Perez (Cuevas-Perez I), 640 F.3d 272, 286 (7th Cir. 2011) *cert. granted, judgment vacated*, 132 S. Ct. 1534 (U.S. 2012).
[78] *Id.* at 272.
[79] Cuevas-Perez v. United States (Cuevas-Perez II), 132 S. Ct. 1534 (2012).
[80] *Id.*
[81] *In re Askin*, 47 F.3d 100, 105-06 (4th Cir. 1995).
[82] *Id.* at 106.
[83] *Graham*, 846 F. Supp. 2d at 389-90.

that "if the arc of technological improvement . . . should be altered in a way that does infringe a person's legitimate expectation of privacy, the solution is properly for the legislature to address."[84]

Legislators should heed the judicial call and construct a new measure that both protects location data privacy and serves as a test case for comprehensive reform of privacy legislation for all forms of personal data. If such a law were wisely and carefully drafted, it would not only stand as a model for data privacy laws of the future but could become the data privacy law of the future with minor amendments.

II. The Peril of Devotion

The Framers of the U.S. Constitution designed the American legislative process to be slow.[85] Therefore, it does not and cannot keep pace with changes in technology.[86] To make matters worse, legislators and judges barely grasp technology.[87] Yet, legislators cannot abdicate their duty simply because the subject of their effort eludes them in both pace and comprehension.

Current legislation and most legislative proposals to protect personal location data are flawed because either they place excessive importance on the use of certain technologies in generating location data, or they require that the location data be generated in conjunction with a third-party service. For example, the definition of location data put forward by one pair of

---

[84] *Id.* at 390.

[85] Jonathan T. Molot, *The Judicial Perspective in the Administrative State: Reconciling Modern Doctrines of Deference with the Judiciary's Structural Role*, 53 STAN. L. REV. 1, 48-49 (2000).

[86] Mulligan, *supra* note 55, at 1559; *see generally* Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep Up with Technological Change*, 2007 U. ILL. J.L. TECH. & POL'Y, Fall 239 (explaining "why technological change generates legal problems").

[87] *See, e.g.*, discussion of the shortcomings of the *Skinner* decision, *supra* Part I.A.; Statement of Sen. Ted Stevens, Chairman, S. Comm. on Commerce, Science and Transportation, at 9:12 (June 28, 2006), *available at* http://media.publicknowledge.org/stevens-on-nn.mp3 (commenting that "the internet is . . . not a big truck, it's a series of tubes"); Transcript of Oral Argument at 29, City of Ontario, Cal. v. Quon, 130 S. Ct. 2619 (2010) (No. 08-1332) (statement of Roberts, C.J.) ("Maybe—maybe everybody else knows this, but what is the difference between a pager and e-mail?"), *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/08-1332.pdf; In re Application of the United States, 396 F. Supp. 2d 45, 49 (D. Mass. 2005) (acknowledging, in a frank and forthright manner, a "dearth of technological savvy on the part of the [Court]").

commentators claims to be technologically agnostic[88] but curiously only protects a user's location information if a "radio signal" is used to "deriv[e] or otherwise calculat[e]" it.[89] Another example, this time by United States Representative Jason Chaffetz, is similarly flawed. His Geolocational Privacy and Surveillance Act ("GPS Act") only prohibits a person from acquiring another's location data if that data is provided "by or through the operation of any wireless communication device."[90] He defines a "wireless communication device" to be "any device that enables access to, or use of, an electronic communication system or service, remote computing service, or geolocation information service, *if that device utilizes a radio or other wireless connection* to access such system or service."[91] The tether to specific technology in Representative Chaffetz's proposal is in his reliance on a wireless radio connection to a third party service.

The emphasis on certain technologies results in large holes in the regime of protection for personal location data. They may cover data created by current technologies such as GPS, or cell phones, but they cannot cover other current technology to say nothing of leading edge technology still in development, or technology not yet invented.

A. Current Location Technology Not Covered

No one technology is necessary to generate location data, nor is any third-party service required. For thousands of years people have used celestial navigation techniques to fix their position and navigate from point A to point B.[92] Celestial navigation allows persons to determine their position by observing the stars, the planets and other heavenly bodies.[93] The

---

[88] *See* Pell, *supra* note 31, at 151 (calling for a solution that accommodates "the pace of technological change to a degree that renders it a moot consideration in any court's analysis").
[89] *Id.* at 179, 179 n.249.
[90] H.R. 2168, 112th Cong. (2011), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d112:h.r.02168:.
[91] *Id.* (emphasis added).
[92] *See generally*, *History*, CELESTIAL NAVIGATION, http://celestialnavigation.net/history/ (last visited Feb. 4, 2013).
[93] Bill Myers, *Celestial Navigation, What are the Options?*, NAV.ORG, http://www.nav.org/cel/introduction.html

only equipment required to record location data from celestial navigation techniques are a sextant, a clock, a nautical almanac (to determine location),[94] and a pencil and paper (to record it). People still use celestial navigation to chart their location.[95] Granted, those persons are probably few, but nevertheless, there is no principled reason why celestial navigators should not receive the same privacy protection as GPS navigators.

The bigger current technology problem is inertial navigation systems ("INSs"). Briefly, an INS uses sensors to "track the position and orientation of an object relative to a known starting point. . . ."[96] In other words, the INS takes readings from sensors and calculates how far and in what direction the INS device has traveled from a known initial location to derive a current location. An INS uses sensors similar to what some cell phones currently use to know when its screen is rotated,[97] or what a video game controller uses to know when users swings their tennis rackets.[98] INS units can be entirely self-contained,[99] or used in conjunction with a GPS device.[100] When used as a stand-alone device, an INS does not use radio signals to generate location data. Even when used in conjunction with a GPS device, the bulk of the data *could* be generated by the INS component rather than by the GPS component, depending on choices made by the device's designers. In other words, the device could operate entirely without the use of radio signals. When it does, it will fall outside the protection of the existing law and the majority

---

(last visited Feb. 6, 2013).

[94] *Id.*

[95] *See generally*, K. H. Zevering, *Some New Dimensions in Sextant-Based Celestial Navigation Aspects of Position Solution Reliability with Multiple Sights*, 2 INT'L JOURNAL ON MARINE NAVIGATION & SAFETY OF SEA TRANSP., 271 (2008), *available at* http://www.transnav.eu/Article_Some_New_Dimensions_in_Sextant-Based_Zevering,7,104.html

[96] Oliver J. Woodman, *An Introduction To Inertial Navigation* 5 (Univ. of Cambridge Computer Lab., Technical Report No. 696, 2007), *available at* http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-696.pdf.

[97] *A Tracking Device That Fits On The Head Of A Pin*, PHYSORG.COM (Oct. 5, 2010) http://phys.org/news205500249.html.

[98] TAKAAKI SHIRATORI ET AL, CARNEGIE MELLON UNIV., ACCELEROMETER-BASED USER INTERFACES FOR THE CONTROL OF A PHYSICALLY SIMULATED CHARACTER 2 (2008), *available at* http://graphics.cs.cmu.edu/projects/wii/SIGGRAPHAsia2008_wii.pdf.

[99] Woodman, *supra* note 96, at 5.

[100] *Id.* at 33.

of proposed laws.

B. Future Location Technology Not Covered

Although the seeds of GPS technology were sown in the 1950's, it was still the future until 1988.[101] The GPS's constellation of satellites was not complete until 1993.[102] Just a few years later, the technology became firmly entrenched in things like emergency vehicles, truck fleets, shipping tankers and freighters, commercial airplanes, and personal automobiles and watercraft.[103] Today, GPS devices are ubiquitous, but technology does not stop. Who among us can tell in what direction location technology will move next?

The use of brainwaves seems promising. A tongue-in-cheek suggestion to be sure, but not one made solely for the tin foil hat crowd. Currently, scientists can capture brainwaves using non-invasive technology.[104] They can use the captured signals—as they can fingerprints—to identify a person.[105] While there is apparently no proven or practical technology for using brainwaves to locate an individual, scientists are currently working on "the problem."[106] If such a technology were to rise, one can imagine a vast web of installed technology that could replace everyday things like elevator buttons, debits cards, or airport security. Of course, brainwave technology will not generate personal location data any time soon, if ever, but humans are lousy prognosticators.[107] No one has a crystal ball, which is exactly the point of keeping the law

---

[101] Kleppner, *supra* note 11, at 3-5 (detailing the history of GPS technology and timelining selected events in its development). In 1957, the Soviets launched *Sputnik*, on which American scientists performed proof-of-concept tests that eventually gave rise to GPS as we know it. *Id.* Beginning in 1989, the 24 satellites were launched that form the current GPS. *Id.*

[102] *Id.* at 5.

[103] *Id.* at 2-3.

[104] L. Subramani, *Students Create Brainwave Authentication System*, DECCAN HERALD, http://www.deccanherald.com/content/77651/students-create-brainwave-authentication-system.html; (last visited Feb. 4, 2013).

[105] *Id.*

[106] *See id.*

[107] Dennis Crouch & Jason Rantanen, *Tracing the Quote: Everything That Can Be Invented Has Been Invented*, PANTENTLYO (Jan. 6, 2011), http://www.patentlyo.com/patent/2011/01/tracing-the-quote-everything-that-can-be-invented-has-been-invented.html (tracing the quote: "Everything that can be invented has been invented"—

technologically agnostic. If the law codifies a specific technology, like radio signals for example, it faces the immediate risk of gaps in coverage and unintended consequences as technology shifts. To avoid those outcomes, legislation must remain truly technologically agnostic.

III. The Four Dichotomies

There are many possible criteria on which to build a legislative framework for location data protection. Many potential choices are appealing, or even intuitive, at first glance but only four survive scrutiny. All four are dichotomies: (1) The fact of location vs. Location data, (2) Unrevealed data vs. Revealed data, (3) Historical data vs. Prospective data, and (4) Point-in-time collection vs. Durational collection.

A. The Fact of Location vs. Location Data

Does Fourth Amendment protection diminish if the information recorded by a defendant in his "papers[ ] and effects" is publicly available? Put another way: Could the U.S. Government successfully argue a photograph does not receive Fourth Amendment protection because the photograph *depicts* a public place? No, a court would rightly dismiss the argument. The proper Fourth Amendment analysis, first announced in *Katz*, speaks only to the reasonable expectation of privacy in a place searched, without regard for the content of the place searched.[108] By that same logic, protection of electronic data should not diminish merely because it *contains* a certain fact, or category of fact. However, this is not how courts treat location data. Courts conflate the *fact of a person's location* with that person's *location data*.[109] This Note suggests that a person's

---

erroneously attributed to Charles Duell, a former U.S. Commissioner of Patents—to 1899).

[108] *See* Rakas v. Illinois, 439 U.S. 128, 143 (1978).

[109] *See, e.g.*, *Cuevas-Perez I*, 640 F.3d at 275 ("[I]n general: real-time information is exactly the kind of information that drivers make available by traversing public roads."); *Skinner*, 690 F.3d at 775 ("In short, [the defendant] did not have a reasonable expectation of privacy in the data emanating from his cell phone that showed its location.").

location information or *data* should be eligible to receive protection, without regard to whether the underlying *fact of a person's location* is protected.

If we consider the *fact of a person's location* to be that aspect of reality that relates to a person's position on the Earth, and that person's *location information* or *location data*[110] to be such a *fact* reduced to a communicable form or fixed in a tangible medium, then it becomes apparent that while the *fact of a person's location* may be wholly contained within that person's *location data*, the two are distinct and deserving of separate treatment.

While the previous paragraph may appeal to the doctrinaire, it may not be clear. So, an example: imagine the Grand Canyon. Its "geologic color[s] and erosional forms decorate a canyon that is 277 river miles . . . long, up to 18 miles . . . wide, and a mile . . . deep."[111] Those are facts.[112] Now imagine a man standing on a ridge of the Canyon with a cell phone in hand. The erosional forms strike a chord in him and he takes a photograph to preserve the memory of his time with the eighth wonder of the world.[113] He looks at the photograph and sees a three and a half inch reproduction of the geologic colors on his phone's screen. His photo is obviously not the Grand Canyon; it is simply the visible facts of the Canyon recorded in a digital format. Likewise, location data is not location. It is a record of the fact of a person's location. Others may freely access the facts of the Grand Canyon and even the exact spot from which he took his photo, but others may not freely access the photo. The same should hold for location data. The public may be able to freely observe a person while in public, but the public does not in fact—

---

[110] This Note does not need to recognize a distinction between location data and location information. However, one could consider "information" to be unrecorded and "data" to be recorded, analogous to the difference between "work" and "copy" under copyright law. A "work" is an abstraction, an original creation of the author, while a "copy" is a physical embodiment of the work. *See* 17 U.S.C. § 101 (definition of "copies").

[111] *Grand Canyon National Park*, NAT'L PARK SERV., http://www.nps.gov/grca/index.htm (last visited Feb. 5, 2013).

[112] A fact is "[s]omething that actually exists; an aspect of reality. . . ." FACT, BLACK'S LAW DICTIONARY (9th ed. 2009).

[113] Jayne Clark, *The World's 8th Wonder: Readers Pick The Grand Canyon*, USA TODAY (Dec. 22, 2006, 9:03 AM), http://usatoday.com/travel/news/2006-11-23-7-wonders-grand-canyon_x.htm.

and should not in the law—have free access to that person's location data.

B. Unrevealed Data vs. Revealed Data

The second dichotomy recognizes, tailors for the information age, and then incorporates the Third Party Doctrine from the Supreme Court's Fourth Amendment jurisprudence. In *United States v. Miller*,[114] the Supreme Court first announced what is now known as the Third Party Doctrine.[115] In accordance with this doctrine, a person "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[116] In other words, "[b]y disclosing [information] to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed."[117] The Third Party Doctrine is highly controversial,[118] but "firmly entrenched."[119] The Doctrine's flaws are clear, as are its virtues.

Critics of the Doctrine assert that the Court was simply wrong in *Miller*.[120] In *Miller*, the Court held that persons do not have "any legitimate expectation of privacy concerning the information kept in bank records."[121] A critic would say that the expectation of privacy in bank records is indeed reasonable because there is no practical alternative to keeping money in a bank. Critics also assert that the Doctrine grants too much power to the government.[122] It grants virtually unlimited power to take business records, which is fully at odds with the tenants of

---

[114] U.S. v. Miller, 425 U.S. 435 (1976).
[115] Wayne R. LaFave, *Search And Seizure: A Treatise on the Fourth Amendment*, 1 Search & Seizure §2.7(c) (4th ed.).
[116] *Miller*, 425 U.S. at 443.
[117] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).
[118] *Compare* LaFave, *supra* note 115 ("The result reached in *Miller* is dead wrong.") *and* Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 Pepp. L. Rev. 975, 976 (2007) ("The [Third Party Doctrine] was controversial when adopted [and] has been the target of sustained criticism. . . .") *with* Kerr, *supra* note 117, at 561 ("This Article responds that critics have overlooked the benefits of the [Third Party Doctrine] and have overstated its weaknesses.").
[119] Jack I. Lerner & Deirdre K. Mulligan, *Taking the "Long View" on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3, 5 (2008).
[120] Kerr, *supra* note 117, at 587.
[121] *Miller*, 425 U.S. at 442.
[122] *See* Kerr, *supra* note 117, at 587.

limited government and freedom.[123]

Proponents of the Doctrine assert that the *Miller* outcome is correct even if the specific holding is somewhat tenuous.[124] If it is conceded that persons have a legitimate expectation of privacy in bank records, then disclosure to the bank implies consent.[125] Proponents also assert that if the Doctrine does grant too much power, then other legal doctrines successfully restrain it.[126] Where all agree is that the Doctrine strongly affects the balance of public and private interests.[127] The Doctrine's merits mean that it cannot be eliminated, but its demerits mean that it should not be codified as currently understood.

The solution then is to concentrate on the definition of the word "revealed," common to most formulations of the Doctrine. The question, for purposes of this Note, becomes: When should personal information in the hands of a third party be considered revealed? In modern society, one would imagine the spectrum of revelation is anchored on one end by a situation in which a person walks down the street trailed by a 20 foot long rolling billboard that displays that person's social security number in 3 foot tall letters.[128] The other end, one would imagine, is anchored by a situation in which a person manually encrypts digital files and then stores those files with a service that encrypts it yet again.[129] In the first situation, a person—without question—fully reveals his or her information and it would be very difficult to justify a scheme that even tried to apply Fourth Amendment-like protection. In the second, the government probably could not access—as a technical matter—the digital information even if the third party (i.e., the service provider) gave what data it had to the government (i.e., the manually encrypted

---

[123] *See id.*
[124] *See id.*
[125] *See id.*
[126] *See id.* Examples of other legal doctrines are evidentiary privileges and entrapment law. *Id.*
[127] *See id.* at 575.
[128] LifeLock, *Commercial*, YOUTUBE (Feb 6, 2011), http://www.youtube.com/watch?v=jIQ92ZpTDZk.
[129] *See* Melanie Pinola, *How To Add A Second Layer Of Encryption To Dropbox*, LIFEHACKER (June 20, 2011, 6:30 PM), http://lifehacker.com/5794486/how-to-add-a-second-layer-of-encryption-to-dropbox.

files). Of course, most information falls somewhere in the middle of these two extremes. The law must account for as much of the spectrum as possible. It must allow access to information on the revealed end and restrict access to information on the concealed end while giving courts guidance on how to treat information in the middle.

C. Historical Data vs. Prospective Data

The third dichotomy recognizes and largely incorporates the long-held distinction between historical surveillance and prospective surveillance.[130] Historical surveillance, of course, is accessing recorded information about past events. Prospective surveillance is the collection of information as it is generated. Analysis of this dichotomy begins from the premise that the more information that one person knows about another, the greater the invasion of privacy. The importance of this distinction is readily apparent and maintains its vitality in the information age. Historical surveillance is less intrusive than prospective surveillance primarily because historical surveillors know in advance what information is relevant and can collect only that information.[131] On the other hand, prospective surveillors cannot know in advance whether any piece of gathered information is relevant to the surveillor's purpose and thus lawful.[132]

Historical surveillance is less intrusive in a second way. The collection of historical data is necessarily limited to the span of time over which data is retained, while collection of prospective data may be unlimited.[133] A relevant example is provided by retention periods of cellular service providers. In 2010, the U.S. Department of Justice conducted a survey and determined that the surveyed providers maintained cell location information for periods between

---

[130] *See generally*, Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 616-18 (2003).
[131] *Id.*
[132] *Id.*
[133] *See* Kevin McLaughlin, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT L.J. 421, 432 (2007).

four month and two years.[134] Even in the absence of legislated restrictions, cellular service providers have no compelling commercial reason to retain location data indefinitely, so they do not.[135] But, if required by law enforcement to report prospective data, the law enforcement agency could easily maintain that data indefinitely and thus track a person indefinitely.[136]

When it comes to prospective location data, there is an additional complication. Most prospective data will likely be "regularly occurring" data. That is, most data generated will come from the ordinary use of the device that produces the data. Some data however, will be "on demand" data. That is, some data generated will be generated because a service provider made a special request of the device to produce the data.[137] If the service provider placed the special request at the behest of a government agent, a party might argue that the service provider's act is analogous to the trespass that occurred in *Jones*. To date, no federal court has addressed the argument of an intangible trespass in the location data context, but the prospect is intriguing.[138]

D. Point-In-Time Surveillance vs. Durational Surveillance

The last dichotomy, Point-in-time surveillance vs. Durational surveillance, begins from the same premise as the Historical data vs. Prospective data dichotomy. It further recognizes that

---

[134] *Cell Phone Location Tracking Request Response – Cell Phone Company Data Retention Chart*, AM. CIVIL LIBERTIES UNION, http://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart, (last visited Feb 5, 2013) (reporting data retention policies for "Cell towers used by phone," one of the means by which law enforcement agencies track cellular telephones).

[135] *See* Allie Bohm, *How Long Is Your Cell Phone Company Hanging On To Your Data?*, AM. CIVIL LIBERTIES UNION, (Sept. 28, 2011, 10:17 AM), http://www.aclu.org/blog/technology-and-liberty/how-long-your-cell-phone-company-hanging-your-data. Apparently, there is no legislated restriction on retention of location data; otherwise there would be uniformity across cellular service providers. *Id.* In addition, if cellular telephone providers had a compelling commercial reason for maintaining data indefinitely, they would. *Id.* (discussing the data retention policies—as opposed to legal obligations—of major cellular telephone service providers).

[136] It is difficult to find examples of what location data records from cellular service providers look like, but it appears that the amount of information necessary to pinpoint a cellular phone at a given time is very small, and thus maintaining records over long periods of time is possible. *See Training Materials for Tracking Cellphones*, N.Y. TIMES 5 (Mar. 31, 2012), http://www.nytimes.com/interactive/2012/04/01/us/celltraining_documents.html (providing an example from AT&T of location records in a slide entitled "Call Detail Records ATT Example").

[137] *See supra* Part I.A (discussing the Sixth Circuit's *Skinner* decision)

[138] And outside the scope of this Note.

longer periods of surveillance can paint a more complete picture of a person's movements and thus are more intrusive than shorter periods of surveillance.

The dichotomy positions point-in-time surveillance against durational surveillance because the two differ in kind, not merely degree. Whereas varying durations differ merely in degree. To illustrate, take as an example ordinary police work at the scene of a bank robbery in 1980.[139] Without raising substantial privacy concerns, police collect information from observant persons or publically positioned—not necessarily publically owned or operated—recording devices available at the time and place in question. Surveillance of a more substantial duration of any given person is more extraordinary in these moments. This dichotomy seeks to grant the same abilities and limitations while allowing police to take advantage of the modern technological advancements.

The attempt to analogize to historical methods, however, does not result in a perfect fit. The two situations do differ in that taking a person's personal location data will affirmatively disclose the person's device's location. Whereas, speaking with studiously observant persons or viewing publically positioned recording devices has a more limited chance of success. For this reason, point-in-time surveillance still needs some procedural checks.

E. Content Data vs. Non-Content Data and Why It Should Be Disregarded

Many possible dichotomies exist that could form the basis of personal location data protection scheme. Only four are important enough to codify; they are discussed above.[140] Notable for its absence from the list is the Content Data vs. Non-Content Data dichotomy. It is a fixture in most discussions of the Fourth Amendment and is historically significant. Therefore, it warrants some discussion. As will be made clear, this dichotomy has outlived its usefulness and

[139] In 1980, personal location services and data were not yet ubiquitous. *See supra* Part I.B.
[140] *See supra* Parts III.A–D.

should be omitted from any future location data legislation.

The Supreme Court's current Fourth Amendment jurisprudence establishes a distinction between "content" data and "non-content" data.[141] Content data is protected while non-content data is not.[142] Congress incorporated this distinction into the ECPA.[143] The ECPA defines the "content" of a communication to "include[] any information concerning the substance, purport, or meaning of that communication."[144] However, as discussed above, the ECPA is a difficult law to understand and apply in light of other complications.[145] The good news is that Congress can and should discard the content versus non-content dichotomy.

The distinction first arose in 1877, in *Ex parte Jackson*.[146] In 1877, it was illegal to send information about lotteries through the mail.[147] The petitioner in *Ex parte Jackson* was convicted of doing just that.[148] The only piece of evidence against him was a letter that he mailed to another man in New York.[149] The Court opined that "[l]etters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form . . . as if they were retained by the parties . . . in their own domiciles."[150] The dichotomy is significant in the world of physical communication because the government must take an additional, intrusive step—beyond viewing the outside of the letter or sealed package—in order to access the "content" of the communication. Namely, it must open the "letter" or the "sealed package." The information on the outside is readily observable. This additional, intrusive step is

---

[141] United States v. Hambrick, 225 F.3d 656, at *4 (4th Cir. 2000).
[142] *Id.* at *4.
[143] *See* 18 U.S.C.A. § 2510(8) (West 2002).
[144] *Id.*
[145] *See supra* Part I.B.
[146] Ex parte Jackson, 96 U.S. 727 (1877); *see also* Walter v. United States, 447 U.S. 649, 654 (1980) (suggesting that *Ex parte Jackson* established the principal that sealed articles of mail may not be opened without a warrant); *Applying the Fourth Amendment*, *supra* note 18, at 1022.
[147] *Ex parte Jackson*, 96 U.S. at 727.
[148] *Id.*
[149] *Id.* at 727, 737.
[150] *Id.* at 733.

critical. As *Ex parte Jackson* makes clear, there is a difference "between what is intended to be kept free from inspection . . . and what is open to inspection. . . ."[151] Among the things intended to be kept free from inspection are "letters, and sealed packages."[152] Among the things open to inspection are "newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined."[153] The two groups vary only in the fact that present in the first group is a physical barrier between the inside and outside of the communication. However, no analogous barrier is present in most modern era contexts

Commentators nevertheless identify an analogy between email and snail mail.[154] The analogy is informative because on the surface, it seems like a good fit, but ultimately it fails. As suggested, there is so-called "header information" in an email.[155] Header information is roughly akin to the address information on a physical letter. Its purpose, among other things, is to reveal to the carrier, the identity of the sender and the recipient such that the carrier can properly deliver the email. There is also the body of the email. The body of the email is very much akin to the letter itself (absent the envelope); it is the information that the sender is conveying to the recipient. Typically, the sender does not intend that the carrier see this part of the email. It is then suggested that header information should be considered non-content data and the body should be considered content data. But, here is the failure: if a person has access to the header information of an email, they also have access to the body of the email—one is not sealed from the other. Header information is merely delimited from the body by lines of text. It is not compartmentalized in such a way that an additional, intrusive step must be taken to get from the

---

[151] *Id.*
[152] *Id.*
[153] *Ex parte Jackson*, 96 U.S. at 733.
[154] *See, e.g.*, *Applying the Fourth Amendment*, *supra* note 18, at 1022-23. Snail mail is a piece of physical mail sent through the U.S. Postal Service. *Snail Mail*, DICTIONARY.COM, http://dictionary.reference.com/browse/snail+mail (last visited Feb 5, 2013).
[155] *Applying the Fourth Amendment*, *supra* note 18, at 1023.

"non-content" portion of the email (i.e., the header information) to the "content" portion of the email (i.e., the body). This is so unlike a physical letter that the analogy fails. A far stronger analogy is between an email and a postcard.[156] If any part of a postcard is available for inspection, the whole postcard is available for inspection.

While the letter analogy fails, at least it presents a clear—if ultimately illusory—line of demarcation between content and non-content data in the email context. The same cannot be said in the location data context. The content/non-content conclusion varies by device, turning on the purpose for which the device generates location data. Courts often find location data generated by services as a byproduct (e.g., cell phone services), to be non-content information.[157] On the other hand, data generated by services for which location data is the heart of the service (e.g., GPS-capable devices and GPS location data, "ping" data possibly qualifies here too), would seem to be content data under the ECPA.[158]

Another less-discussed but still important aspect of *Ex parte Jackson* is that the letter in question was sent through the U.S. Postal Service.[159] In other words, it was placed directly into the hands of the federal government, against whom the Fourth Amendment guards. Email does not operate that way. Typically, email only passes through privately owned equipment and never touches government hands (rather, equipment). This raises the question: Even under the email-letter analogy, when would the government, in *Ex parte Jackson*-like fashion, have access to the

---

[156] *E.g.*, Donald R. Lundberg & Jeffrey S. Goens, *Ready, Aim, Disclose: Understanding the Power of the Email "Send" Button in Your Law Practice*, 55-MAR RES GESTAE 30, 31 (2012); LAWRENCE ROGERS, CARNEGIE MELLON UNIV., EMAIL: A POSTCARD WRITTEN IN PENCIL 1-2 (2001), *available at* http://nwl.cc/email_postcard.pdf (analogizing unencrypted email to a postcard).

[157] *E.g.*, In re Application of the United States, 396 F. Supp. 2d 747, 758 (S.D. Tex. 2005); In re Application of the United States, 402 F. Supp. 2d 597, 600 (D. Md. 2005); In re Application of the United States, 509 F. Supp. 2d 76, 80 (D. Mass. 2007).

[158] There does not appear to be any federal case law on point, but the definition given for the content of a communication "includes any information concerning the substance . . . of that communication." 18 U.S.C.A. § 2510(8) (West). When a person uses a GPS device, the only information exchanged is location data and the time. Therefore, because the user is not looking to get the time from the GPS devide, the "substance . . . of that communication" can only be the location data. *See* Kleppner, *supra* note 11, at 4.

[159] *Ex parte Jackson*, 96 U.S. at 727.

information "open to inspection"? Under even the lowest legal hurdle imaginable, the government would have to go to the private entity to take the email. The government would otherwise not have access of any kind. Should this taking be viewed as an intrusive step, akin to opening the letter in *Ex parte Jackson*? If it is viewed as the intrusive step, would that mean that the entire email—header information and all—is "content"? These questions are not easy to answer and are outside the scope of this Note. They are raised here only to make clear how ill-fitting the content/non-content distinction is in the information age. The analogy is simply no longer useful.

IV. A Legislative Proposal

Armed with the understanding that legislators should avoid memorializing current technology, we can better understand the focus of what we seek to protect.[160] The law must focus on and protect user location data. It should not protect *cell phone* location data, *GPS* location data, or the location data resulting from any other specific technology.[161] Personal location information is worthy of protection regardless of the form in which it is generated, or the technological age in which it is generated. It should incorporate those aspects of Fourth Amendment jurisprudence that best balance personal privacy with public interests and discard the rest.

Because the chief concern of this Note is location data privacy, it makes sense to produce a comprehensive definition of location data that establishes the boundaries of the proposal.

---

[160] *See supra* Part II.

[161] Therefore, we can disregard as unimportant the nature or identity of the device that aids in generating the information, the nature or identity of the infrastructure that transports the information from point to point, the nature or identity of the infrastructure that stores the information, and the length of time information is stored, whether by an intermediary or terminal entity. We should also avoid references to the precision of the involved technology. Current technology is already accurate and only getting more accurate. *STMicroelectronics Enables "The Next Step" in Precision 3D Location Sensing*, STMICROELECTRONICS (Sept. 5, 2012), http://www.st.com/internet/com/press_release/p3325.jsp.

Conceptually, the definition will cover traditional and non-traditional uses of established and future technology. Also, the definition will cover location information at the point of *generation*. No distinction will be made between broadcast and recorded location information, or transmitted and non-transmitted information.

The secondary purpose of this Note is to convince the reader that implementing measures to protect personal location data could serve as a test bed for the larger goal of establishing a coherent protection scheme for all personal data. To that end, erecting a firewall between the current legislation "protecting" personal data from the proposed legislation to protect personal location data becomes important. An effective firewall requires a precise definition of location data. In the future—provided the test is successful—this firewall becomes moot. Personal location data then becomes but one prong of a personal data definition.

A. Definitions Peculiar To Location Data

Up until this point, this Note has discussed a person's location data, but in reality, a person cannot generate location data in the absence of a device, whether that device is the state of the art, or the lowly pencil. Regardless of the technology involved, location data can only capture a device's location—yes, including brainwave technology—and only by extension, a person's location. Knowing that, the legislative framework begins with the following proposed definitions:

1. The "fact of a device's location" is that aspect of reality that relates to the device's position on the Earth.
2. "Location data" is the fact of a device's location reduced to a communicable form or fixed in a tangible medium.
3. "Personal location data" is any location data generated using any method now

known or later developed[162] by, or in conjunction with, any device owned or operated by a user that establishes the absolute or relative position of that device.[163]

These definitions accomplish two things. First, they codify the first of the four proposed, important dichotomies.[164] Second, they exclude data generated "by, or in conjunction with, any device" *not* "owned or operated by a user" from the definition of personal location data.

The second is significant because it preserves the legal reasoning behind the *Knotts* line of cases. As previously discussed, *Knotts* dealt with the location data generated by a police-operated tracking device planted in a barrel of liquid used to make methamphetamine.[165] The Court held this method of monitoring a person's location did not violate the defendant's Fourth Amendment rights.[166] Because the police operated (and presumably owned) the device, the *Knotts* line of cases will remain intact even after these definitions pass into law.

B. Definitions Applicable To All Data

The remaining proposed dichotomies need not be specific to location data. In order to codify them, additional definitions are necessary:

4. "Revealed" data is that which is (1) given by a person to the public or to any other person indiscriminately, (2) generated solely by a person, or in conjunction by the person with one or more third parties, and provided by the

---

[162] The helpful phrase "any method now known or later developed" is borrowed from the very forward-looking, and technologically agnostic, Copyright Law of 1976. 17 U.S.C. § 101 (2010) (definition of "copies" and "phonorecords").

[163] The astute reader will recognize that my brainwave surveillance example from Part II.B. will probably fall outside this definition of personal location data. That is unless a user owns or operates the brainwave scanners that are generating the location data. However, the point earlier was merely that brainwave technology has a plausible use in generating location data, not that that specific application of the technology should create personal location data subject to protection.

[164] The Fact of Location vs. Location Data. *See supra*, Part III.A.

[165] *Knotts*, 460 U.S. at 277-79.

[166] *Id.* at 285.

person to a third party for the purpose of the third party's interaction, or (3) generated solely by one or more third parties.

5. "Unrevealed" data is that which is not revealed.

These two definitions establish the default position of the law, which is to consider information unrevealed unless specifically considered revealed by Congress. Three bodies of information are "revealed" under this definition. Body (1) covers the rolling billboard example[167] and includes any information that a person has indisputably revealed. Body (2), for example, will consider revealed dialed telephone digits and email addresses sent through an email service. It would not consider revealed the words spoken during a phone call or the subject line of an email. A person does not speak words or provide the subject line to a third party so the third party may interact with them. The service merely carries them from the sender to the recipient. Mere possession of information by a third party or simple carriage of information by the third party would not reveal the possessed/carried information under this definition. Nor will information generated in conjunction with a third party automatically be considered revealed. Significant in the location data context, cell tower records and GPS records because both require a user device and third party service. Body (3) will consider revealed information like credit card records and utility records. Body (3) probably does not have much significance in the location data context.

Incorporating the Historical data vs. Prospective data dichotomy does not require any novel definitions, but for the sake of completeness:

6. "Historical" surveillance is the retrieval of data generated over a period of time prior to the initial request for the data.
7. "Prospective" surveillance is the retrieval of data that includes any data generated over a period of time subsequent to the initial request for the data.

[167] *Supra*, Part III.B.

The definitions used to implement the Point-in-time surveillance vs. Durational surveillance dichotomy require some judgment. Of course, the number of categories and the bounds of each are somewhat arbitrary and thus subject to a policy determination by Congress. Here is one possible set of definitions:

8. "Point-in-time" surveillance is the retrieval of data generated over a period of time equal to or shorter than 1 minute.
9. "Short-term" surveillance is the retrieval of data generated over a period of time longer than 1 minute but equal to or shorter than 120 hours.
10. "Long-term" surveillance is the retrieval of data generated over a period of time longer than 120 hours but equal to or shorter than the statutory maximum.

C. Category Matrices

Below are the category matrices first mentioned in the introduction. They attempt to make visual the relative importance of each of the four important dichotomies. They then offer a measure of importance, relative to the other data categories and thus give life to the remaining dichotomies.

Historical

	Revealed	Unrevealed
Point-in-Time	**Very Low**	**Low**
Short Duration	**Low**	**Medium**
Long Duration	**Medium**	**High**

Prospective

	Revealed	Unrevealed
Point-in-Time	**Low**	**Medium**
Short Duration	**Medium**	**High**
Long Duration	**High**	**Very High**

V. Conclusion

Modern technology has moved American society beyond the point where the Supreme Court is willing to extend Fourth Amendment protection. Current federal legislation attempts to fill the privacy gap but is anachronistic and obsolete. The personal location data context presents a clear example of the importance of this issue. Without intending the result, Americans have allowed their personal technology to become tracking devices. It is time for Congress to recognize the importance of the issue and enact far-sighted and comprehensive legislation that is technologically agnostic and cognizant of four important dichotomies. The legislative framework suggested by this Note will restore the privacy/security balance envisioned by the Fourth Amendment for the foreseeable future.