REBUILDING BRIDGES: ADDRESSING THE PROBLEMS OF HISTORIC CELL SITE LOCATION INFORMATION

Mark Daniel Langer[†]

In February 2010, the FBI began a massive manhunt for the two men responsible for over fifteen bank robberies in Arizona and Colorado.[1] When surveillance tapes and eyewitness accounts did not provide the necessary information to identify the suspects and regional law enforcement had been unable to determine their identities,[2] FBI agents turned to the historic cell site location information ("CSLI") that cell phone service providers had collected from towers around the banks.[3] Using a § 2703(d) court order ("D Order"),[4] the agents collected nearly 150,000 cell phone numbers that were in the vicinity of four of the banks at the time of the robberies.[5] Out of this information, the FBI agents quickly isolated the two numbers that reappeared, and by March 11, agents had arrested the two suspects.[6]

This is just one example of how government agents can use historic CSLI in a criminal investigation, but it explains, at least in part, why privacy advocates are concerned.[7] A court authorized D Order can produce a vast amount of information for government agents. As cell phone technology develops, businesses increase the amount of information they collect, which then increases the amount of information the government can demand. The debate about historic CSLI is far from settled, and this dissonance highlights a meaningful debate regarding the reach of the third-party doctrine.[8] Further,

† J.D. Candidate, 2014, University of California, Berkeley, School of Law.

1. *See* Nate Anderson, *How "Cell Tower Dumps" Caught the High Country Bandits—and Why It Matters*, ARS TECHNICA (Aug. 29, 2013, 5:00 AM), http://arstechnica.com/tech-policy/2013/08/how-cell-tower-dumps-caught-the-high-country-bandits-and-why-it-matters.

2. *See id.*

3. *See id.*

4. 18 U.S.C. § 2703(d) (2012). The requirements and justification of D Orders will be discussed in detail *infra* Section I.A.

5. *See* Anderson, *supra* note 1.

6. *See id.*

7. *See, e.g.*, *In re Historic Cell Site Location Information*, EPIC (Dec. 20, 2013), https://epic.org/amicus/location/cell-phone-tracking.

8. *See infra* Part I.C.

given recent developments that have challenged and minimized the usefulness of other criminal investigatory tactics like GPS tracking,[9] government agents are likely to fight for their ability to collect CSLI against demands for reform.

Yet, a spirited discussion of reform still surrounds the government's use of D Orders to obtain historic CSLI, as many reformers and legal scholars argue that the government is reaching too far into the lives of individuals.[10] However, many of the potential solutions to this problem face considerable obstacles: the Supreme Court seems hesitant to act;[11] Congress is considering a number of reforms, but these might not be successful in the present political environment;[12] and state legislatures, although often more willing to protect privacy, are not equipped to provide adequate protection from government agents.[13]

Using a recent Fifth Circuit opinion to present these issues, this Note begins by discussing the background to this area of criminal surveillance law. It then seeks to shift the focus away from specific technologies and toward the parties caught up in the debate, arguing that the goal of reformers should be to develop better relationships among the government, businesses, and individuals. Strengthening these relationships would foster an environment better suited to face the future problems that technology will pose—specifically on historical cell site location information.

Part I of this Note provides background information on the key criminal surveillance laws, the Electronic Communications Privacy Act ("ECPA") and the Stored Communications Act ("SCA"); the technology behind and use of historic CSLI; and the development of the third-party doctrine. Part II delves into the recent Fifth Circuit opinion on the constitutionality of using a court order, instead of a warrant, to collect historic CSLI from service providers. It then discusses the criticism of the government's expansion of the third-party doctrine with historic CSLI and the potential harms to the individual and the

9. *See* United States v. Jones, 132 S. Ct. 945, 949 (2012) (holding that placing a GPS tracker on defendant's car qualified as a trespass).

10. *See, e.g.*, Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 702–705 (2011); Erin Murphy, *The Case Against the Case for the Third Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239 (2009); Lior J. Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010 (2013); 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 (2012).

11. *See infra* Section III.B.

12. *See infra* Section III.C.

13. *See infra* Section III.D.

relationships between government agents, businesses, and individuals arising from such an expansionistic view. Part III describes the search for a solution and the merits of the various avenues for reform. Part IV outlines a number of ways to use historic CSLI reform to balance these relationships and provide a healthier environment for future technological developments.

I. BACKGROUND

To assess the Fifth Circuit opinion in *In re Application of the United States of America for Historical Cell Site Data* ("*In re Cell Site*"),[14] its criticism, and potential solutions, a basic understanding of the applicable law and technology is necessary. This Part discusses the statutory framework of ECPA, the technology behind CSLI, and the third-party doctrine, which constitute the core of *In re Cell Site*.

A. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

ECPA provides structure and unification to how government agents treat electronic information. It consists of three parts: the Wiretap Act,[15] regulating the interception of electronic communication; the Pen Register Act,[16] regulating the collection of telephone metadata; and the Stored Communications Act,[17] regulating the collection of information in electronic storage. ECPA regulates how government agents can collect such information, providing varying levels of protection for each different type of information.

Although much of ECPA has met criticism, the SCA is the source of some of the most heated debates.[18] The Stored Communications Act, as the name implies, covers electronic communications that are stored by a service provider, including the substantive content such as emails and non-substantive content like email metadata.[19] The SCA, in § 2703, sets out the

14. *In re* Application of the United States of America for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) [hereinafter *In re* Cell Site].

15. 18 U.S.C. §§ 2510–2522 (2012).

16. 18 U.S.C. §§ 3121–3127 (2012).

17. 18 U.S.C. §§ 2701–2712 (2012).

18. It goes without saying that at least certain parts of ECPA are in need of reform. As the Electronic Frontier Foundation notes, Attorney General Eric Holder also supports reform. *See* Nate Cardozo & Mark M. Jaycox, *Even Attorney General Eric Holden Supports ECPA Reform*, EFF (May 23, 2013), https://www.eff.org/deeplinks/2013/05/even-attorney-general-eric-holder-supports-ecpa-reform. Now, after nearly thirty years, Congress is seriously considering ECPA amendments, particularly to the statute's treatment of emails. *See, e.g.*, Online Communications and Geolocation Act, H.R. 983, 113th Cong. (2013).

19. 18 U.S.C. §§ 2701–2712 (2012).

general requirements that must be followed for a government agent to compel the disclosure of stored information.[20] This information can include electronic communications in storage, electronic communications in a remote computing service, and records concerning either electronic storage or remote computing.[21] Historical CSLI, as electronic information in the files of service providers, falls under this last category of electronic storage.

18 U.S.C. § 2703(c) provides multiple avenues to compel disclosure of records. The first and most obvious way to compel disclosure would be with a search warrant,[22] but the SCA also allows such compulsion with a D Order as laid out in § 2703(d).[23] Section 2703(d) requires that an officer provide "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[24] The requirement that the information merely be relevant and material to an ongoing investigation allows government agents to collect a wide array of information. Although not an insignificant hurdle for criminal investigations, it is less than the probable cause requirement of a search warrant or the "super warrant" requirement of the Wiretap Act.[25]

There are two more elements of § 2703 that bear mentioning, though the Fifth Circuit decision does not discuss them in detail. First, the SCA does not provide a notice requirement for information that government agents produce through § 2703(c).[26] Second, government agents may request that a company preserve the records in question pending a court order.[27] These elements do not have to do with the justification of a D Order and thus are of less interest with regard to the Fifth Circuit's opinion. However, these elements will be relevant to the later discussion about how the current legal framework has affected the landscape and potential solutions.

---

20. § 2703.

21. *Id.*

22. *See* FED. R. CRIM. P. 41.

23. 18 U.S.C. § 2703(d) (2012). For an example of a 2703(d) application and court order, see *Sample 18 U.S.C. §2703(d) Application and Order*, FEDERAL JUDICIAL CENTER, http://www.fjc.gov/public/pdf.nsf/lookup/CompIn01.rtf/$file/CompIn01.rtf (last visited Feb. 24, 2014).

24. § 2703(d).

25. The Wiretap Act places even more limitations on collection on top of probable cause such as minimizing the amount of intercepted information and requiring that other investigative procedures be tried first. *See* 18 U.S.C. § 2518(3).

26. 18 U.S.C. § 2703(c)(3) (2012).

27. § 2703(f)(1).

B. CELL SITE LOCATION INFORMATION

1. Technology

To discern the potential problems of the use of historic cell site information, it is helpful to isolate it from other geolocational data, especially GPS data. Cell phone service providers collect CSLI whenever a cell phone connects to a cell tower.[28] When a cell phone is in contact with a cell tower, both when making and receiving a call, its interaction with the closest cell towers is recorded, thus providing potentially real-time location information about the cell phone holder.[29] Unlike a GPS device, a cell phone is not necessarily constantly connected to a cell tower, so reconstructing a suspect's steps is not quite as simple or accurate.[30] What is more, the precision of the location information varies from region to region. Cell phone towers can service a cell phone that is up to twenty-one miles away.[31] However, highly populated areas require many more cell towers to manage the traffic. Thus, populous cities will often have many towers and thus provide more exact geolocational information.[32] A cell tower network in some cities can provide a cell phone location accurate to within fifty meters.[33]

2. Use

Government agents have been quick to make use of historic CSLI in criminal investigations.[34] In part, this is because of the recent holding in *United States v. Jones*.[35] In *Jones*, the Supreme Court held that placing a GPS tracking device on a car without a warrant constituted a trespass and therefore was an unreasonable search.[36] While the Court specifically avoided the issue of whether the use of GPS tracking, especially in the long term, could qualify as a search, Justices Sotomayor and Alito at least expressed

28. *See* Freiwald, *supra* note 10, at 702–05.

29. *See id.*

30. *See id.*

31. *See* WAYNE JANSEN & RICK AYERS, GUIDELINES ON CELL PHONE FORENSICS: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 63 (Natl. Inst. Stand. Technol. Spec. Publ. 800-101, 2007), *available at* http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf.

32. *See* Pell & Soghoian, *supra* note 10, at 128.

33. *See id.*

34. *See* David Kravets, *After Car-Tracking Smackdown, Feds Turn to Warrantless Phone Tracking*, WIRED (Mar. 31, 2012, 5:13 PM), http://www.wired.com/threatlevel/2012/03/feds-move-to-cell-site-data.

35. United States v. Jones, 132 S. Ct. 945 (2011).

36. *Id.* at 946.

their doubts about the propriety of using tracking technology this way.[37] Since *Jones*, the FBI has stopped a large number of its GPS tracking procedures and significantly increased its requests for CSLI.[38]

CSLI comes in many different categories. First, it can be either prospective or historical.[39] Because historic CSLI is information that cell phone providers have already collected and logged, it seems intuitively less problematic than prospective monitoring. Second, CSLI can contain multiple types of information, including, inter alia, initiation information (where the cell phone started a call), termination information (where the cell phone ended the call), and duration information (where the cell phone was throughout the duration of the call).[40]

CSLI can also contain logging information. Government agents can create this information through a pinging process, by calling cell phones just long enough to create a log in a company's records. However, courts might inquire as to whether the government engaged in such a practice before deciding to grant a D Order.[41] In *In re Cell Site*, the government agents asked for all historic CSLI within a certain period,[42] and the court did not address whether the government agents involved used pinging to increase their information.

C. THE THIRD-PARTY DOCTRINE

In arguing for the constitutionality of using a D Order to disclose geolocational information, both the government and legal scholars rely heavily on the third-party doctrine.[43] To understand the third-party doctrine, it is important to first understand its context within Fourth Amendment law. The Fourth Amendment protects "against unreasonable searches and seizures."[44] Given the language of the Fourth Amendment, it becomes important to discern what qualifies as an unreasonable search.

---

37. *Id.* at 957 (Sotomayor, J., concurring); *id* at 964 (Alito, J., concurring).

38. *See* Kravets, *supra* note 34. It is important to note that the FBI's shift in procedure does not mean that the use of CSLI is as accurate or invasive as the use of GPS tracking devices. Typically a D Order is less controversial and less difficult to procure, thus giving government agents incentive to focus first on CSLI before seeking GPS information under a warrant requirement.

39. *See* Freiwald, *supra* note 10, at 698.

40. *See id.* at 702–705.

41. *See id.*

42. *In re* Cell Site, 724 F.3d 600, 602 (5th Cir. 2013).

43. *See, e.g.*, Brief for the United States at 33–34, *In re* Application of the United States of America for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) (No. 11-20884), 2012 WL 604860.

44. U.S. CONST. amend. IV.

The Supreme Court provided its general test for an unreasonable search in *Katz v. United States*.[45] In *Katz*, the defendant was convicted of "transmitting wagering information by telephone."[46] To catch him, the police attached an electronic recording device on top of a public phone booth he used and monitored his phone calls.[47] The Supreme Court held that, although this was a public place, Katz had a reasonable expectation of privacy in his communications.[48] Justice Harlan, in his concurring opinion, fleshed out the reasonable-expectation-of-privacy test.[49] The test consists of two prongs: (1) whether the individual had a *subjective* expectation of privacy, and (2) whether that expectation of privacy is one that society is *objectively* willing to accept as reasonable.[50] Justice Harlan argued that the facts of the case satisfied the test, as Katz had the subjective intent, and society recognized an objective expectation of privacy in the phone booth.[51] Since this decision, Justice Harlan's two-prong test has proven to be the foundational test for unreasonable search claims.

Although *Katz* provides an example of an expectation of privacy that society is willing to consider reasonable, not every expectation of privacy will be reasonable. The third-party doctrine is one instance in which one does not have a reasonable expectation of privacy. The Supreme Court firmly established this doctrine in two cases, *United States v. Miller* and *Smith v. Maryland*.

In *Miller*, the defendant brought a Fourth Amendment challenge against the government's use of the defendant's bank records and information.[52] The Court held that the defendant did not have a protectable Fourth Amendment interest in the bank's business records.[53] Because the bank was a third party, and the business records in question pertained to a transaction of which the bank was a party, the Court held that the bank was able to share the information that the defendant had provided to it.[54] The Court noted that individuals do not have a reasonable expectation of privacy in information that they provide to third parties.[55] The Court found this to be true,

45. Katz v. United States, 389 U.S. 347 (1967).
46. *Id.* at 348.
47. *Id.*
48. *Id.* at 359.
49. *Id.* at 361.
50. *Id.*
51. *Id.* at 361–62.
52. United States v. Miller, 425 U.S. 435, 438–39 (1976).
53. *Id.* at 440.
54. *Id.* at 443.
55. *Id.*

regardless of whether the "information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[56]

The Supreme Court continued to bolster the third-party doctrine in *Smith v. Maryland*.[57] In *Smith*, the government used the information from a telephone company's pen register to review the phone numbers that the defendant had been calling.[58] Although the defendant claimed a Fourth Amendment interest in his phone calls and phone call information, the Supreme Court again found no Fourth Amendment protection.[59] Just like the bank records of *Miller*, the Supreme Court held that an individual voluntarily provided pen register information to the third-party telephone company.[60] Even if this is information in which the defendant subjectively expected privacy, society was not willing to accept that expectation as reasonable.[61]

II. THE *IN RE: APPLICATION OF THE UNITED STATES OF AMERICA FOR HISTORICAL CELL SITE DATA* DECISION

A. HISTORY

In October 2010, government agents filed three § 2703(d) applications under the Stored Communications Act.[62] The applications asked for sixty days of historical cell site data, as well as other subscriber information.[63] The magistrate judge granted the request for subscriber information but requested a brief justifying the historical cell site data applications.[64] After examining the brief, the magistrate judge then declared that under Supreme Court precedent, compelled warrantless disclosure of cell historical cell site data violates the Constitution.[65] The government brought the case before the federal district court, which also held that the standard under the Stored Communications Act was below constitutional requirements.[66]

56. *Id.*
57. Smith v. Maryland, 442 U.S. 735 (1979).
58. *Id.* at 737.
59. *Id.* at 745.
60. *Id.* at 742.
61. *Id.* at 742–44.
62. *In re* Cell Site, 724 F.3d 600, 602 (5th Cir. 2013).
63. *Id.*
64. *Id.*
65. *Id.*
66. *Id.*

B. ANALYSIS

1. Textual Argument

Before the Fifth Circuit could decide on the constitutionality of using a D Order for historic CSLI, it had to first address the argument by the American Civil Liberties Union ("ACLU")[67] that such an analysis would be unnecessary. Constitutional interpretation issues, especially those surrounding the Fourth Amendment, can be extremely controversial, and court precedent has developed a "canon of constitutional avoidance" that enables courts to avoid interpreting an issue so as to raise a constitutional question.[68] When applying this canon to statutory interpretation, courts must "first ascertain whether a construction of the statute is fairly possible by which the constitutional question may be avoided."[69]

The ACLU argued that just such an interpretation was possible, relying upon an interpretation of the SCA that arose in a Third Circuit case on the very same matter.[70] According to the ACLU, the SCA is ambiguous as to when warrants are required to obtain certain information from third parties.[71] Section 2703(d) states that a D Order "may be issued" by a competent court.[72] This language is permissive, implying that judges are able to use discretion when providing a D Order. Also, the statute clearly states that an order shall be provided "only if" the government meets the requirements of the D Order, namely, making a specific and articulable showing that the records are relevant to an ongoing criminal investigation.[73] The ACLU, and the Fifth Circuit dissent, argued that the best interpretation of this language

67. The ACLU has created a campaign focused on protecting the rights of individuals in the digital age. *See Protecting Civil Liberties in the Digital Age*, ACLU, https://www.aclu.org/protecting-civil-liberties-digital-age (last visited Mar. 9, 2014). The issue of warrantless cell phone tracking continues to be an important concern for them. *See Warrantless Cell Phone Location Tracking*, ACLU, https://www.aclu.org/technology-and-liberty/warrantless-cell-phone-location-tracking (last visited Mar. 9, 2014).

68. Clark v. Martinez, 543 U.S. 371, 381 (2005).

69. United States v. Sec. Indus. Bank, 459 U.S. 70, 78 (1982) (internal quotation marks omitted) (quoting Lorillard v. Pons, 434 U.S. 575, 577 (1978)).

70. *See In re* United States for an Order Directing a Provider of Elec. Commc'n. Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010).

71. Brief of the American Civil Liberties Union Foundation, the ACLU Foundation of Texas, the Electronic Frontier Foundation, the Center for Democracy and Technology, and the National Association of Criminal Defense Lawyers as Amici Curiae in Support of Affirmance, *In re* Application of the United States of America for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) (No. 11-20884), 2012 WL 1029813, at *8–9 [hereinafter ACLU Brief].

72. 18 U.S.C. § 2703(d) (2006).

73. *Id.*

is that the order "may not issue unless the standard is met."[74] If that interpretation is correct, then there might also be times when judges can require more than the minimal specific and articulable facts standard.

Although this interpretation of the statute is not unreasonable, the majority of the Fifth Circuit held that it was incorrect.[75] The majority focused its interpretation not on "only if" but on the "shall issue" part of the text.[76] Under this interpretation, the words "may issue" merely permit courts of competent jurisdiction to issue such orders while the phrase "shall issue" compels judges to provide the order if the government can meet the specific and articulable facts requirement.[77] This argument did not satisfy the dissent,[78] but it allowed the majority to proceed to the constitutionality issue.

2. Reasonable Expectation of Privacy vs. Third Party Argument

Because magistrate judges do not have discretion, the Fifth Circuit had to decide the constitutionality of the D Orders in this context.[79] It began by noting the two distinct questions that the ACLU and the government addressed. The ACLU looked at *which types of information* are collected and analyzed the D Orders based on Supreme Court's precedent on tracking devices.[80] The government looked at *who is collecting* the information and analyzed Supreme Court precedent on business records.[81]

Ultimately, the Fifth Circuit concluded that the government approached the issue correctly.[82] Although the ACLU brought up important concerns with tracking cases such as *United States v. Jones*[83] and *United States v. Karo*,[84] those cases hinged on the fact that the government was the agent collecting the information and tracking the people in question.[85] With historic cell site data, cell phone companies collect the information as part of ordinary business records. Therefore, the court noted that the Supreme Court's precedent on third-party business records, such as *Smith v. Maryland* and

74. *In re* Cell Site, 724 F.3d 600, 619 (5th Cir. 2013) (Dennis, J., dissenting).
75. *Id.* at 608.
76. 18 U.S.C. § 2703(d).
77. *In re Cell Site*, 724 F.3d at 608.
78. *Id.* at 616.
79. *Id.* at 608.
80. *Id.* at 609–10.
81. *Id.*
82. *Id.*
83. United States v. Jones, 132 S. Ct. 945 (2011).
84. United States v. Karo, 468 U.S. 705 (1984).
85. *In re Cell Site*, 724 F.3d at 609.

United States v. Miller, applied. These cases say that as long as the *business* collects the information, the government will be able to use a D Order.[86]

Although this distinction convinced the court, the court discussed two other factors that could potentially influence the third-party doctrine. First, it highlighted the transactional analogy presented in *United States v. Warshak*.[87] In *Warshak*, the Sixth Circuit held that the government could not compel disclosure of internet service providers' records when they included the content of emails.[88] In those circumstances, the provider was merely an intermediary between two communicating subscribers, not a party to the transaction.[89] In *In re Cell Site*, however, the consumer sent the cell site information to the service provider alone, which gave the company every right to both collect the information and provide it to the government. Second, the ACLU expressed concern that consumers did not provide this information voluntarily because they did not know the provider would collect it.[90] The Fifth Circuit held that cell phone users sufficiently know how their information is collected and use their phones voluntarily.[91] Further, the court noted that even if a consumer's reasonable expectation of privacy had shifted, it would be for Congress to reevaluate the statute, not the courts.[92]

C. ANALYSIS OF THE FIFTH CIRCUIT DECISION

The third-party doctrine is not without its critics. Although these critics might disapprove of the third-party doctrine in general, like the use of undercover investigators, the use of the historic CSLI demonstrates a new problem that arises as the government applies the third-party doctrine to new types of technology. This Note focuses specifically on how the third-party doctrine is being applied to CSLI. There are two main critiques that apply to the expansion of the third-party doctrine by the Fifth Circuit to historic cell site information, one practical and one doctrinal, and this Section discusses each in turn.

1. The Practical Critique

The practical argument against the expansion focuses on one primary aspect of the third-party doctrine: the idea that an individual *knowingly* and

86. *See* discussion *supra* Section I.C.
87. *In re Cell Site*, 724 F.3d at 611.
88. United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010).
89. *Id.*
90. ACLU Brief, *supra* note 71.
91. *In re Cell Site*, 724 F.3d at 613.
92. *Id.* at 614–15.

voluntarily supplies her information to a company. In *Smith*, the Supreme Court held that the defendant knowingly released the information.[93] It argued that, with early telephones, one would speak directly to an operator, and this operator counted as a third party, just like the bank teller in *Miller*.[94] Even though telephone companies no longer used human beings as operators, the Court believed that a telephone user would still know that she would be giving the pen register information to the telephone company to make a phone call.[95]

This argument seems to make sense in *Smith*, and the Fifth Circuit held that the same logic holds true with CSLI today. The majority held that cell phone customers should know that their CSLI will be collected and potentially disclosed.[96] Customers with common sense would probably know that a cell phone company would have to relay their call through the nearest cell tower, thus potentially providing information about their whereabouts.[97] Even if customers do not know this information, the majority noted that cell phone service providers mention this information collection in their terms of service agreements.[98]

However, this interpretation is not altogether convincing.[99] First, although the operator analogy used in *Smith* makes sense, as the phone user is speaking directly with another human being, the analogy breaks down as technology gets more and more complex. It is not likely that the average cell phone user understands how call-relay technology works or the types of information that a cell phone service provider might be collecting. Further, it is also not clear that a user should be assumed to know and understand how his or her information is collected because of the information in a contract. In real life, customers often do not read the fine print of the contract terms.[100] Courts are still willing to find these types of agreements valid, as

93. Smith v. Maryland, 442 U.S. 735, 742–43 (1979).

94. *Id.* at 745.

95. *Id.* at 743 ("Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes.").

96. *In re Cell Site*, 724 F.3d at 613.

97. *Id.*

98. *Id.*

99. *See, e.g.*, ACLU Brief, *supra* note 71 (arguing generally against this knowledge and voluntariness assumption).

100. *See* Rainer Böhme & Stefan Köpsell, *Trained to Accept? A Field Experiment in Consent Dialogs*, 2010 PROC. SIGCHI CONF. ON HUM. FACTORS COMPUTING SYS. 2403, 2405 ("More than 50% of the users take less than 8 seconds [to read the entire end user license agreement], which is clearly too short to read the entire notice.").

well as click-through or shrink wrap agreements, because it is of a practical necessity for contract law and helps both parties create the transaction they want.[101] But with the risk of potential criminal liability instead of merely civil liability, courts should probably be more careful when assuming what a customer does or does not know about how the technology works. This problem will only intensify as technology increases in complexity.

2. The Doctrinal Critique

Both Susan Freiwald and the ACLU also argue that the expansion of the third-party doctrine is not supported by recent judicial decisions. They point to Justice Sotomayor's concurring opinion in *United States v. Jones*, where she noted that the third-party doctrine should not have the same role today as it did in days of simpler technology.[102] These scholars also look to the Sixth Circuit's decision in *Warshak*.[103] In *Warshak*, the Sixth Circuit held that subscribers have a Fourth Amendment right of privacy in their emails.[104] This went against the guidelines of the SCA. Critics use these new cases to show a growing trend of reading the third-party doctrine more narrowly than the government's interpretation and being extremely careful when extending the reach of government surveillance through new technological tools.[105]

3. Response to the Third-Party Doctrine Critics

Although the critics of the third-party doctrine provide strong arguments for why it should not be applied, there are also strong arguments in favor of the doctrine.[106] One of the strongest arguments in favor of the third-party doctrine is its simplicity and technologically neutral nature.[107] The third-party doctrine provides government agents with a clear model for when individuals have a reasonable expectation of privacy. If the information has been given to another person, it loses its reasonable expectation of privacy without need

101. *See* ProCD v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996).

102. United States v. Jones, 132 S. Ct. 945, 957 (2011) (Sotomayor, J., concurring).

103. United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010).

104. *Id.* at 283–88.

105. *See, e.g.*, Freiwald, *supra* note 10, at 700–01. The Ninth Circuit had a similar holding against the SCA.

106. Orin Kerr is one of the strongest supporters of the third-party doctrine. In 2009, the Berkeley Technology Law Journal held a symposium that included a discussion of Orin Kerr's work on the third-party doctrine. *See* Murphy, *supra* note 10; Richard Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199 (2009); Orin Kerr, *Defending the Third-Party Doctrine: A Response to Epstein and Murphy*, 24 BERKELEY TECH. L.J. 1229 (2009).

107. *See generally* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).

of extensive fact-finding. Also, the third-party doctrine does not favor any specific type of technology. It applies equally to everyone. A problem with most alternatives to the third-party doctrine is that they necessarily focus on some types of technology, be it cell towers and CSLI or GPS tracking. Critics might not have a problem with certain third-party information (like subscriber information, for example), but they do have a problem with certain types of information and specific uses of the information (like the extended tracking issues raised by Justice Alito in *Jones*).[108] Alternatives applying a less universal approach would pose serious problems for government agents, as it simply would not be clear until an appellate court decision just where on the sliding scale of surveillance their actions landed.

D. THE HARMS OF THE CURRENT APPROACH

Assessing the harms of privacy violations is no simple task. By their nature, these types of harms are more ethereal than the average tort or crime. Other articles discuss the harms of privacy violations in-depth,[109] and although a full discussion of the nature of historic CSLI and its potential for misuse exceeds the scope of this Note, two specific types of harms merit discussion. The first type of harm is the archetypal privacy harm: the pervasive effects of government surveillance on individual development and activity. The second harm is the harm to the relationships between the government, businesses, and individuals.

1. Pervasive Effects of Government Surveillance

Because privacy harms rarely have an immediate or obvious physical, emotional, or financial impact on an individual, it can be difficult to isolate exactly what the harms are and how they arise. The classic privacy harm derives from the fear of an all-seeing government. Scholars have likened this harm to "Big Brother" from George Orwell's *1984*, or Bentham's *Panopticon*.[110] In either case, authority figures have complete knowledge of the activities of the individuals under their control, and the knowledge that the government is watching has a profound impact on how individuals go about

108. United States v. Jones, 130 S. Ct. 945, 964 (2012) (Alito, J., concurring) ("But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.").

109. *See* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011) (discussing the types of privacy harms and their effects on the individual). *See also* Pell & Soghoian, *supra* note 10, at 163–74.

110. *See* Pell & Soghoian, *supra* note 10.

their daily lives.[111] Although these examples are perhaps a little drastic, they help flesh out our intuitions about privacy harm and isolate potential harms, though perhaps on a smaller scale.

Unfortunately, these discussions of privacy harms are difficult and often philosophical, and they do not provide a clear and compelling reason why individuals should be concerned about potential privacy risks.[112] Although they might not be enough for an individual customer to change his or her mind when purchasing something like a cell phone, it is hard to argue that these privacy fears are completely unjustified. A Big Brother-type government or Panopticon used on innocent people seems intuitively wrong, and the Constitution has protections in place to keep the government from becoming this kind of power.[113]

2. *Harm to Relationships Between Government Agents, Businesses, and Individuals*

Proving convincing privacy harm can be difficult, but expanding the third-party doctrine to a broader array of information has also had other effects on society. The current regulatory framework covers three parties: government agents, businesses, and individuals. As technology gets more complex, with companies collecting more information and government agents compelling disclosure of more information, political and economic pressure have begun to fracture these relationships.[114]

The relationship between government agents and businesses is perhaps the relationship most affected by the expansion of the third-party doctrine and the increasing richness of metadata collection by businesses. As mentioned in Section I.B.2, *supra*, government agents have significantly increased the number of requests for historical CSLI.[115] They have also increasingly been cracking down on companies that do not comply with their

111. *Id.* In both of these examples, the authority figures use a lack of privacy to exert control on individuals.

112. *See* Calo, *supra* note 109.

113. *See, e.g.*, U.S. CONST. amend I & V (including free speech and due process clauses).

114. Clearly this type of harm is not caused solely by the expansion of the third-party doctrine and the government's use of historic CSLI. There are many factors to blame outside of this specific legal area, such as customer apathy, aggression by individuals in the government or business sector, and economic pressures. However, the fact that there are multiple factors to blame for the state of these relationships does not mean that improvements in this area should be avoided. Even if one disagrees that the third-party doctrine and CSLI is the cause of these unhealthy relationships, new approaches to these ideas can still be part of the solution.

115. *See* Kravets, *supra* note 34.

requests.[116] This type of activity shifts the power in favor of government agents and increases the likelihood that a business will surrender customer information without a fight.

At the same time, individuals have no clarity regarding what government agents can do and are doing when it comes to compelling businesses to turn over records. The SCA does not require disclosure of this type of information,[117] and as more and more information falls under the SCA, individual customers become increasingly ignorant as to how and when their information is being used. This lack of transparency fosters apathy in individuals, the majority of whom are not aware of how their information is being used, and decreases the possibility that individuals can successfully seek change through a democratic process.

If individuals are ignorant about what government agents are doing, they are just as ignorant about how businesses are collecting and storing their information. This is partly due to the new complexities that arise with technological developments. It is difficult to clearly explain how businesses collect information and how that information might be used.[118] However, when paired with the pressure that businesses receive from government agents, businesses lose any incentive to share their businesses practices with customers. Thus, there is a lack of accountability to customers about what types of information a business collects, how it releases that information, and how long it keeps that information. Customers lose any bargaining power or accountability that they might have.

III. THE SEARCH FOR A SOLUTION

As described in Section II.C, *supra*, the government's use of a D Order to obtain historic CSLI has been met with resistance and criticism. Some scholars and judges have provided their own solutions to the problem, most of which fall into a handful of different camps. The first, a direct counter to *In re Cell Site*, would provide magistrate judges with more discretion to decide whether a D Order suffices. Another solution to the problem would be for the Supreme Court to decide on this issue once and for all. Although this

116. *See infra* text notes 156–157 and accompanying text.

117. *See supra* note 26 and accompanying text.

118. For example, when Google and Facebook updated their privacy policies in 2012, a survey found that the changes to the policies were too confusing for customers to understand. *Survey Finds Facebook and Google Privacy Policies Even More Confusing Than Credit Card Bills and Government Notices*, SIEGEL+GALE (Apr. 24, 2012), http://www.siegelgale.com/media_release/survey-finds-facebook-and-google-privacy-policies-even-more-confusing-than-credit-card-bills-and- government-notices.

would provide a more concrete solution, others have argued that any solution should arise under broader ECPA reform. And one final solution is simply for states to decide for themselves what to allow within their borders, which would at least limit the extent of the problem. This Part discusses each of these solutions in turn, outlining the potential solution as well as the pros and cons of each. Two central problems reoccurring in these solutions are that (1) they would each require a dramatic change to the current state of affairs and (2) often their focus is not technologically neutral.

A. MAGISTRATE JUDGE DISCRETION

As mentioned in the discussion of *In re Cell Site*, the text of the SCA allows for multiple interpretations.[119] Discounting the argument of the ACLU,[120] the Fifth Circuit held that the SCA requires that a magistrate judge issue a D Order as long as the government meets the requirements as outlined in§ 2703(d). In other words, as long as the government offers "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[121] However, the Third Circuit decided a similar case differently.[122] According to the Third Circuit, § 2703 allows for discretion on the part of the magistrate judge.[123] The court held that if Congress had meant for judges not to have any discretion, it could have clearly limited their authority.[124] Such an interpretation could alleviate much of the concern with the government's use of a D Order to compel historic cell site information. Although the government would still be able to collect historic CSLI without a warrant, there would be an extra layer of protection for individuals in the form of satisfying the magistrate judges' own standard. This is not as dramatic as requiring a warrant in all circumstances, but it is a step in that direction.

While this solution could potentially provide more protection than the current surveillance regime, it faces some strong criticisms. The first problem is that it eliminates the certainty that government agents have when pursuing

119. *See supra* Section II.B.

120. ACLU Brief, *supra* note 71.

121. 18 U.S.C. § 2703(d) (2012).

122. *See In re* United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (2010).

123. *Id.* at 319.

124. *Id.* ("We respectfully suggest that if Congress intended to circumscribe the discretion it gave to magistrates under § 2703(d) then Congress, as the representative of the people, would have so provided.").

a D Order. No longer will government agents know what will be necessary to receive the information they need because, instead of a clear statutory requirement, they must meet the subjective standard of the particular magistrate judge from whom they are requesting the order. This problem is compounded by the fact that the Third Circuit does not provide a standard for the magistrate judges to evaluate when to require a warrant in place of a D Order.[125] Some, if not most scholars, would agree that the limitations placed on government agents should be clear if they are to be effective.[126] This type of subjectivity would appear to encourage jurisdiction shopping, assuming that not all magistrate judges have the same penchant for privacy protection.

Judge Dennis, in the dissent to *In re Cell Site*, noted one more problem with giving magistrate judges discretion to require a warrant.[127] The dissenting opinion focused on the importance of constitutional avoidance.[128] This doctrine, which has been reinforced by the Supreme Court,[129] requires courts to avoid constitutional questions when at all possible. The dissent noted that giving magistrate judges discretion would simply move the broad constitutional analysis to a fact-intensive analysis of any particular D Order.[130] Not only does such a decision ignore the doctrine of constitutional avoidance, Judge Dennis argued that ex parte application proceedings provide a poor forum for Fourth Amendment analysis.[131]

B. SUPREME COURT ACTION

Another way to address the use of historic CSLI would be through a Supreme Court holding. The Supreme Court could simply decide that the disclosure of location information should require a warrant, not merely a D Order. Given the existing circuit split on this issue, there is a good chance that there also will be circuit splits on other third-party doctrine issues as well. These types of splits might be difficult for the Supreme Court to ignore. A Supreme Court holding could limit the third-party doctrine in multiple

125. *Id.*

126. *See* Pell & Soghoian, *supra* note 10, at 175; Orin Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373 (2013).

127. *See In re* Cell Site, 724 F.3d 600, 617 (5th Cir. 2013) (Dennis, J., dissenting) (desiring a holding "that does not require magistrates to speculate on societal expectations in ex parte application proceedings devoid of the concrete investigative facts upon which Fourth Amendment analysis depends").

128. *Id.* at 616–17.

129. *See id.* (citing Zadvydas v. Davis, 533 U.S. 678, 689 (2001)).

130. *Id.* at 630–31.

131. *Id.*

ways. It could limit the disclosure of location information with a warrant requirement, or it could eliminate certain types of information collection by adhering to the mosaic theory of surveillance.[132]

Unfortunately, those looking to the Supreme Court for an answer to the third-party doctrine, especially as it relates to technological issues like historic CSLI, might have a long wait. In *City of Ontario v. Quon*, the Supreme Court showed that it did not like to use a fact-specific case to develop "far-reaching" technology policy decisions.[133] The Supreme Court continued in this vein in *United States v. Jones*.[134] In *Jones*, the court had the opportunity to take a strong position on long-term GPS tracking.[135] Although Justice Sotomayor, in her concurring opinion, was critical of the use of long-term GPS surveillance,[136] as well as the third-party doctrine in a technology setting, the Supreme Court intentionally avoided any specific holding on the subject, instead focusing on the physical trespass committed by the government agents through the surveillance.[137] It seems apparent that the Supreme Court is hesitant to make the kind of decision that many reformers seek; however, Chief Justice Roberts has mentioned the importance of seeking a solution to the technological challenges now facing the United States.[138]

C. ECPA REFORM

Although there are multiple avenues for reform, much of the scholarly debate has centered around ECPA reform.[139] Unlike the Supreme Court, which specifically seeks to avoid far-reaching policy decisions in the technology field,[140] Congress has the ability, and arguably the duty, to address these issues. In enacting ECPA in 1986, the Congressional Committee

132. Justice Alito alludes to the mosaic theory in his discussion of long-term surveillance. United States v. Jones, 130 S. Ct. 945, 961 (2012) (Alito, J., concurring). This is a separate issue that will not be discussed in full here. However, for an interesting discussion of the mosaic theory, compare David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628 (2005) with Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

133. City of Ontario v. Quon, 560 U.S. 746, 759 (2010).

134. *Jones*, 132 S. Ct. 945.

135. *Id.*

136. *Id.* at 955 (Sotomayor, J., concurring).

137. *Id.* at 946–47.

138. Robert Barnes, *Supreme Court May Rule on Cellphone Privacy*, BOSTON GLOBE (Aug. 11, 2013), http://www.bostonglobe.com/news/nation/2013/08/10/supreme-court-may-decide-how-private-cellphone-supreme-court-may-decide-how-private-cellphone/PpNnx3uSelQbHteZbSsiKP/story.html.

139. *See* Pell & Soghoian, *supra* note 10 (focusing on what a new legislative framework should be); Kerr, *supra* note 126.

140. City of Ontario v. Quon, 130 S. Ct. 2619, 2629–30 (2010).

Report noted the importance of Congress's role in ensuring that privacy protections remained in place in the face of technological developments:

> The law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.[141]

It seems safe to say that the technological developments surrounding smart phones, including the extended reach of government surveillance, is part of that "gradual erosion." If so, it would appear that Congress not only has the ability, but also the duty to address the issue per its own mandate.

There are two other reasons why congressional reform would be a good approach to this issue. First, any changes to ECPA would not have to be limited to the facts of a case, like a Supreme Court opinion. That means that Congress does not have to wait for a case with perfect facts, and it can address issues as broadly or specifically as it wants. Second, Congress also has the ability to develop a more complete response to technology concerns with a statutory amendment.

Congressional reform might seem like the best possible solution to the technology problem, but it still faces multiple issues of its own. First, Congress has recently been stuck in a stalemate between the government and interest groups. If Congress finds it difficult to find a compromise on a budget even with the threat of government shutdown,[142] it seems unlikely that it will be able to address difficult and controversial privacy issues. This is especially true as current reformers in the debate often present extreme changes to ECPA.[143] Privacy interest groups are often quite frustrated with the current state of the law and that can lead to demands for dramatic reform. However, this type of dramatic reform will not go without a fight. This is especially true in the area of historic CSLI. Since the Supreme Court's holding in *Jones*, which made the use of GPS tracking more difficult for

141. S. REP. NO. 99-541, at 2 (1986).

142. *See* Lori Montgomery & Zachary Goldfarb, *President, Congress leave one crisis behind but face long road to budget deal*, WASH. POST (Oct. 17, 2013), http://www.washingtonpost.com/business/economy/president-congress-leave-one-crisis-behind-but-face-long-road-to-budget-deal/2013/10/17/4e4eda14-3767-11e3-ae46-e4248e75c8ea_story.html.

143. *See, e.g.*, Press Release, Senator Rand Paul, Sen. Paul to Introduce Fourth Amendment Restoration Act of 2013 (June 6, 2013), http://www.paul.senate.gov/?p=press_release&id=838. Senator Paul's draft of the Act, which would require a warrant to search the phone records of Americans, is available at http://www.paul.senate.gov/files/documents/4thAmdtRestoration.pdf.

government agents,[144] the government's use of D Orders has increased astronomically.[145] It is hard to imagine that the government would allow reform to ECPA's D Orders without a fight.

Furthermore, although Congress has been able to make some specific changes to technological developments in privacy law, such as the Video Privacy Protection Act,[146] these changes have been few and far between. Congress enacted ECPA in 1986, and it has taken nearly thirty years for Congress to consider changing its position on the protection of emails. Although some might take encouragement from the fact that privacy concerns have made headlines recently,[147] it is by no means certain that this will lead to congressional action concerning historical CSLI. If anything, other privacy matters are more pressing, and less difficult, than historic CSLI and geolocational information. If Congress were to pass privacy legislation, it would make sense for it to address these more politically pressing concerns first.

D. STATE-SPECIFIC SOLUTIONS

The federal government is not the only sphere where reformers have sought change in the collection of cell phone location information. In July 2013, the New Jersey Supreme Court unanimously held that law enforcement agents in New Jersey must have a warrant to obtain location information from cell phone providers.[148] This is not the first time that states have led the way in protecting privacy. For example, states have led the way with regard to data breach notification law.[149] Moreover, multiple states have a right to privacy as part of their constitution,[150] whereas the U.S. Constitution does not specifically mention a right to privacy. This constitutional right to privacy could allow more state supreme courts to rule in favor of consumer privacy or more state legislators to pass laws that more strictly enforce privacy rights.

144. United States v. Jones, 132 S. Ct. 945 (2012).

145. *See* Kravets, *supra* note 34.

146. Video Privacy Protection Act, 18 U.S.C. §2710 (2006).

147. *See, e.g.*, *Edward Snowden*, THE GUARDIAN, http://www.theguardian.com/world/edward-snowden (last visited Feb. 24, 2014) (collecting all of *The Guardian* articles relating to Edward Snowden and U.S. government surveillance leaks).

148. *See* Kate Zernike, *New Jersey Supreme Court Restricts Police Searches of Phone Data*, NEW YORK TIMES (July 18, 2013), *available at* http://www.nytimes.com/2013/07/19/nyregion/new-jersey-supreme-court-restricts-police-searches-of-phone-data.html?pagewanted=all.

149. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 171–84 (2d ed. 2013).

150. *See* CAL. CONST. art. I, § 1; MONT. CONST. art. I, § 10.

State privacy solutions could be useful for multiple privacy concerns, but they might not be as successful when it comes to the government's use of historic CSLI. One problem is the nationwide scope of large cell phone companies. Although a state government might not allow agents to force companies in its state to disclose the information, the information might not actually be in the protected jurisdictions. Also, even though some states are willing to bolster privacy protections for individuals, there are many other states, even those that have been strong privacy supporters, which are not likely to make the types of changes seen in New Jersey and Montana.[151]

It is also important to note that criminal investigations are fundamentally different from state-championed data breach laws, and the reasons why differing data breach laws work might not apply to differing surveillance laws. Much like international privacy law, companies can choose to adhere to the law of the strictest jurisdiction (i.e. the European Commission's 1995 Data Protection Directive for broader information privacy law or California law for data breaches).[152] Once a business has the infrastructure in place to handle stricter requirements, much of the economic incentive for avoiding stricter privacy requirements fades away. However, that sort of economic benefit does not apply in this case. The government has in place the ability to obtain a warrant for historic CSLI, but having the ability does not make it any more desirable to government agents to use the warrant method and overcome its higher burden requirements. Also, it is one thing to expect a business to absorb the cost of privacy protection, but quite another to expect government agents to limit criminal investigations. Finally, having fifty different laws for government agents to follow would reduce the efficiency of criminal investigations, and it would probably be most desirable to keep this reform in a federal forum.

IV. SMALL STEPS: BUILDING AN ENVIRONMENT FOR SUCCESS

Although the previous Part outlines potential solutions to the current government use of historic CSLI, none of these solutions will be an easy

151. *See* Hanni Fakhoury, *Governor Brown Vetoes California Electronic Privacy Protection. Again.,* EFF (Oct. 1, 2012), https://www.eff.org/deeplinks/2012/10/governor-browns-vetoes-california-electronic-privacy-protection-again (noting that in California, Governor Brown vetoed a bill that would require a warrant for locational information).

152. *See* Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31; CAL. CIV. CODE § 1798.82 (West 2014).

answer to the problem, and often for similar reasons. Some of the solutions seek changes that are too extreme or far-reaching. This can be a problem with demanding a Supreme Court holding that will significantly change the current Fourth Amendment doctrine and technology landscape, as well as with seeking a new version of ECPA that would eliminate the third-party doctrine or require warrants for all types of information. Even the idea of giving magistrate court judges discretion in deciding the necessity of warrants for CSLI will necessarily cause a dramatic change in the Fourth Amendment legal landscape. If not too extreme, some of the solutions could be too technologically specific. For example, a Supreme Court ruling on the use of historic CSLI might be helpful for awhile, but such specific holdings might become obsolete as soon as they are made.[153]

No matter what solution, or combination of solutions, reformers manage to implement, there will be one more obstacle: an unhealthy environment based on unhealthy working relationships among the government, businesses, and individual consumers. The relationships among these parties have not fared well under the government's approach to historic CSLI, but the blame for this should not rest solely on government's shoulders. Bolstering the balance of power in these relationships and rebuilding the environment surrounding these third-party doctrine issues are vital for future development. Current solutions addressing issues such as historic CSLI will not be perfect, but any problems they may contain will be exploited in an unhealthy environment. As technology advances, an unhealthy relationship among the parties will only hinder healthy adaptation. This Part takes a closer look at each of the individual relationships.

A. GOVERNMENT AND BUSINESSES

In 2007, Albert Gidari, Jr., gave the keynote address at a privacy symposium at the University of San Francisco Law School.[154] Entitled *Companies Caught in the Middle*, the address presented the perspective of the service providers as they stand on the front lines in the battle for privacy.[155] Since September 11, 2001, government agents have had less patience with service providers.[156] By questioning the government's authority or taking time to consider a government agent's request, companies are at risk of being

153. See Kyllo v. United States, 533 U.S. 27, 33–34 (2001) (mentioning the problem of technology changing and holdings becoming obsolete).

154. Albert Gidari, Jr., *Companies Caught in the Middle*, 41 U.S.F. L. REV. 535 (2007).

155. *Id.*

156. *See id.* at 541.

convicted of criminal contempt.[157] After years of being treated like "piñatas,"[158] companies have learned that it is easier to comply with government requests than challenge them. This is especially true when government access can be achieved without notifying the customer.

This was the state of affairs in 2007, and one would hope that the situation has improved over the last six years. This might be true, but without meaningful change in ECPA or Supreme Court holdings,[159] or evidence of a decrease in government access requests, the burden of proof should be on the scholar arguing that the situation has improved, rather than the scholar arguing that the status quo has remained unchanged. Although the government's relationship with businesses can hardly be characterized as healthy, there are multiple ways to begin rebuilding a healthy environment without the large-scale changes often suggested in CSLI reform demands.

1. Costs for D Orders

One way companies might seek to rebalance the power in their relationship with the government is by continuing to charge the government for access to their information. ECPA gives service providers the ability to demand compensation for the costs incurred by responding to government requests, including D Orders.[160] According to statute, this amount must be mutually agreed upon by the government entity and the service provider or decided by a court.[161] Companies take different approaches to reimbursement. For example, Facebook has stated that it might not demand compensation for government requests if they assist in protecting its own interests and customers.[162] Multiple companies have a simple list of costs for each type of information requested.[163] There is no uniform system for deciding these costs.

157. *See id.*

158. *Id.* at 535.

159. Some Supreme Court cases have affected the government's current actions. For example, *United States v. Jones* limited the government's use of GPS tracking. *See* United States v. Jones, 132 S. Ct. 945 (2012). However, this holding only increased the government's reliance on the third-party doctrine and CSLI. *See* Kravets, *supra* note 34. So even pro-privacy developments do not appear to actually help the current relationships between the government and business.

160. 18 U.S.C. § 2706 (2012).

161. § 2706(b).

162. *Information for Law Enforcement Authorities*, FACEBOOK, https://www.facebook.com/safety/groups/law/guidelines (last visited Feb. 24, 2014).

163. Andy Greenberg, *These Are The Prices AT&T, Verizon and Sprint Charge For Cellphone Wiretaps*, FORBES (Apr. 3, 2012, 3:01 PM), http://www.forbes.com/sites/andygreenberg/2012/04/03/these-are-the-prices-att-verizon-and-sprint-charge-for-cellphone-wiretaps; *see*

The flaw with this system is that government agents might not actually be charged for the information that they receive. This might occur because companies make the choice not to pursue reimbursement.[164] It also might occur because technological advances could reduce or eliminate the cost to the companies of complying (e.g., automatic responses). Some might argue that it would not be good to inhibit a government investigation by requiring payment, even when a company is willing to absorb the costs or the costs are negligible. However, privacy advocates have called for a requirement that government agents must pay fees for collecting information.[165]

There are a few strong reasons for requiring the government to pay fees for its collection of customer information. First, it would provide more transparency to the government's actions. By charging the government agents for its services, companies create a paper trail that helps keep track of the amount and types of government actions. Currently this information is not typically available to the public, but if these payment requirements were paired with more freedom for companies to disclose government requests, it would help the public see how much information the government collects. Second, it would ensure that the government has at least some purpose for requesting the information. If such requests for information were free, there would be no incentive to submit narrow requests or not to collect the information at all. Requiring at least some charge for this information would require government agents to think twice before collecting it.[166]

2. *Anti-pinging Requirements*

Another small reform that could help bring more balance to this relationship would be for magistrate judges to officially address the government's use of "pinging." Pinging occurs when government agents call a cell phone and then hang up before the cell actually starts to ring.[167] Doing this creates a log in the cell phone service provider's record, and these logs

also Yahoo! Compliance Guide for Law Enforcement 12, http://pacinlaw.us/pdf/sup/Yahoo_Compliance_Guide.php (last visited Feb. 24, 2014).

164. *See supra* note 162.

165. *See, e.g.*, Anne Flaherty, *What the Government Pays to Snoop on You*, USA TODAY (Jul. 10, 2013, 8:30 AM), http://www.usatoday.com/story/money/business/2013/07/10/what-government-pays-to-snoop-on-you/2504819 (noting Christopher Soghoian's belief that it is better to charge money to create a paper trail).

166. The idea of a company providing information for free is especially problematic, given that a company is going out of its way to encourage government requests for information. This is especially ironic as it is the customer's money that pays for the disclosure.

167. *See* Freiwald, *supra* note 10, at 704.

become historic CSLI within milliseconds after the company receives it.[168] Technically, government agents could regularly ping a suspect as many times as they want before demanding the historic CSLI from a service provider, and thus they can map a suspect's movements as thoroughly as they want. Magistrate judges often push back against "pinging" when it comes to D Orders.[169] They are perfectly equipped to prevent this type of overreach by the government; they could refuse a request if agents engaged in pinging, or they could require government agents to affirm that they did not ping the device for which they now are requesting historic CSLI.

B. BUSINESSES AND INDIVIDUALS

Unlike the relationship between the government and businesses, which is between two powerful and informed parties, customers typically do not have knowledge of how companies use their information or the power to influence a company's decision. Also, unless the information at issue relates to a specific subset of information, like credit reports or health information, there are not many statutes that govern how a company collects and maintains information from an individual. To achieve more balance in this relationship, change will have to come through contractual agreements and increased consumer awareness.

1. Contractual Agreements

Without specific government regulation or customer influence, companies have been able to create contracts that give them free and extensive use of information. To create a change, customers can push for contractual agreements that provide more protection for their information. Without a legislative regulation, one could argue that this is a fruitless discussion, as customers do not have the bargaining power to demand any contractual changes. However, a recent study of consumer opinion by the Berkeley Center for Law and Technology shows that seventy-four percent of consumers believe that cell phone service providers should either not keep their information at all or keep it less than a year.[170] This shows an existing demand for privacy from consumers, a demand that is not likely to decrease given the national attention privacy issues, especially government surveillance, have received. Companies might want to ignore calls for greater

168. *See* Gidari, *supra* note 154, at 543.

169. *See* Freiwald, *supra* note 10, at 704 n.141.

170. Jennifer Urban, Chris Jay Hoofnagle & Su Li, *Mobile Phones and Privacy* 19 (UC Berkeley Pub. Law Research Paper Series, Paper No. 2103405, 2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405.

privacy protections, but it would be foolish to completely ignore consumer opinion.[171] For this reason, at the very least, a discussion of contractual protections for information is worthwhile.

There are many ways that a contractual provision could better protect customer information. One of the easiest ways to protect the information is to include a data minimization requirement in a contract. Currently, telephone service providers do not have limitations on how long they can retain customer information. According to the ACLU's research in 2011, telephone service providers vary in how long they retain customer information, though most keep historic CSLI between one to two years.[172] This is much longer than what many customers might expect or want.[173] Such a minimization requirement might be the easiest way to avoid abuse of historic CSLI.

2. Consumer Awareness

Another important way to help restore the relationship between businesses and customers is to create more consumer awareness. Consumers especially should know how their information will be collected, used, and retained by a company. Most of this type of information is in that company's privacy policy. These privacy policies are often long and complicated, and they do not always contain all the information a customer would want to know. For example, Verizon's Privacy Policy is over 5,500 words long.[174] What is more, it does not say how long it retains information such as historic CSLI, though it does promise to keep sensitive personal information, which is not defined, "only as long as reasonably necessary."[175] A consumer might not know how long is "reasonably necessary" for a company. This is not to single out Verizon for criticism. Nevertheless, when a service provider's

171. This is especially true as privacy is becoming a growing concern for consumers. *See* s.e. Jones, *Why 2014 May Be the Year Consumers Demand Their Privacy Back*, YAHOO! VOICES (Feb. 7, 2014), http://voices.yahoo.com/why-2014-may-year-consumers-demand-their-privacy-12518023.html. In fact, some major companies are using privacy as a selling point. *See* Katy Bachman, *New Microsoft Privacy Campaign Promotes Consumer Control: Campaign Will Stir Debate over Do Not Track*, ADWEEK (Apr. 22, 2013, 6:00 AM), http://www.adweek.com/news/advertising-branding/new-microsoft-privacy-campaign-promotes-consumer-control-148781.

172. *See Cell Phone Location Tracking Request Response – Cell Phone Company Data Retention Chart*, ACLU, https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart (last visited Feb. 24, 2014).

173. *See* Urban et al., *supra* note 170, at 19.

174. *Privacy Policy*, VERIZON, http://www.verizon.com/about/privacy/policy/#wireinfo (last visited Feb. 24, 2014).

175. *Id.*

privacy policy does not mention information like CSLI or give clear timelines for retaining information, customers will be unable to understand how their information is used and act accordingly.

C. GOVERNMENT AND INDIVIDUALS

Many of the individuals' problems with businesses resurface in their relationship with the government. Without transparency, most customers have no reason to know how the government is collecting, using, and retaining their information. To create meaningful change, citizens must have the ability to influence the government's laws, but they cannot do so if they remain unaware of the government's actions. By encouraging the government to increase transparency, individuals will be able to participate more effectively in the political process and bring more balance and accountability to the relationship.[176]

1. Notification for Collection of Information

As written, ECPA does little to encourage transparency on behalf of the government. Although it requires that customers be notified in case of a wiretap,[177] it does not have such a requirement for when companies turn over business records, including CSLI, to the government. When this lack of any notification requirement is paired with an unclear privacy policy, customers have little knowledge of how their information will be used in theory or in practice. By providing a notification requirement for other types of information, customers will be able to see just how often, or not often, their information has been accessed or used. This knowledge will let them make an informed decision on what they would enable the government to do.

Another way to encourage notification, on a broader level, would be to require the government to file reports on how it collects and uses service provider records on the whole. This would not provide the immediate and personal feedback of an individual notification requirement, but it would give privacy advocates and individuals more awareness of current government practices. Congress required these types of reports for wiretaps and pen register trap and trace interception, hoping that it would provide accountability for government activities.[178] The distinction between pen register or wiretap information and other third-party business information makes sense in its historical context. However, these distinctions start to

176. This discussion of government and individual interaction has played an important role in the ECPA reform forum. *See* Pell & Soghoian, *supra* note 10; Kerr, *supra* note 132.

177. 18 U.S.C. § 2703(b) (2012).

178. *See* Pell & Soghoian, *supra* note 10; S. REP. NO. 90-1097, at 69 (1968).

break down in today's smartphone culture. Business records, like historic CSLI, are now much more useful,[179] and much more invasive, than they used to be.

2. Data Minimization

Increasing transparency is not the only way to foster more individual protections. It could also occur with data minimization requirements. The idea of data minimization is not new to ECPA. In the Wiretap Act, law enforcement agents must seek to "minimize the interception of communications not otherwise subject to interception."[180] Currently there is no such minimization requirement for minimizing information collected for other types of information. A minimization requirement could take multiple forms. First, it could require that government agents refrain from collecting information that is irrelevant to an ongoing investigation. It could also require government agencies to discard some of the general information that it collected once it completes an investigation or closes a case.

This second minimization requirement could help to alleviate the concerns that are arising under the mosaic theory. Under the mosaic theory, the government is able to assemble a complete picture of a person's activities through many individual pieces of surveillance.[181] This type of all-compassing surveillance has caused some judicial concern.[182] Although some scholars, notably Orin Kerr, have argued that attacking government surveillance on the basis of the mosaic theory is unconvincing,[183] it could, at least, lend some support to a data minimization requirement. Such a requirement would not need to say that the mosaic theory should limit government surveillance in all respects; it would simply ask that government agents discard information that was not necessary to their investigation.

D. STATE LEGISLATURES ENFORCING MORE INDIVIDUAL PRIVACY RIGHTS

Some state legislatures have already started reforming privacy law and adding more protections than the ECPA requires.[184] These solutions, although not perfect, as they would provide an uneven patchwork of protection for individuals and regulation for companies, can play an

179. *See* Kravets, *supra* note 34.
180. 18 U.S.C. § 2518(5) (2012).
181. *See* Kerr, *supra* note 132, at 313.
182. *See generally* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).
183. *See* Kerr, *supra* note 132.
184. *See supra* Section III.D.

important role in shaping the public discussion and pressuring broader reform. State legislatures have the ability to implement many of the solutions outlined in this Part into their jurisdictions.

V. CONCLUSION

Historic CSLI is a perfect example of how dramatic changes in technology have increased the amount and sensitivity of information that businesses collect from their customers. *In re Cell Site* shows how, under the current constitutional and regulatory framework, courts are willing to expand the third-party doctrine to include this new and sensitive information. The Fifth Circuit's holding allows for an opportunity to reevaluate the flaws in the third-party doctrine and ECPA and to reassess the harms, not just to individuals, but to the relationships between government agents, businesses, and individuals. Any potential solution to this problem should seek to rebuild these relationships, not merely to address the flaws in the regulatory framework, thus providing a healthier environment for future technological developments.