NOTE

PRIVACY IN THE CLOUD: THE MOSAIC THEORY AND THE STORED COMMUNICATIONS ACT

Gabriel R. Schlabach*

In United States v. Jones*, the Supreme Court held that the Fourth Amendment prohibits the government from installing GPS devices on suspects' cars without a warrant. Although the majority limited its holding to the physical installation of such devices, five concurring Justices (including Justice Sotomayor, who joined the majority opinion) indicated their desire for broader privacy protections by endorsing the adoption of the "mosaic theory." Under this theory, certain types of long-term (or otherwise expansive) surveillance violate a suspect's reasonable expectation of privacy, even when each individual act of surveillance would otherwise pass Fourth Amendment muster, because the government can analyze the information in the aggregate to infer private details about the suspect that no individual member of the public could reasonably discover by observing her for a short time.*

While Jones *was limited to GPS tracking, mosaic theory concerns logically extend to a much wider range of new technologies. In recent years, telephone and Internet service providers have amassed extensive (and growing) amounts of data about their customers—more than enough to construct revealing mosaics of these individuals' lives. But under the Stored Communications Act, a component of the Electronic Communications Privacy Act of 1986, the government may order such companies to turn over customers' records using only a court order or an administrative subpoena—less than the warrant and probable cause requirements of a typical Fourth Amendment search.*

Responding to such increasing threats to privacy, this Note proposes an amendment to the Stored Communications Act that would incorporate the mosaic theory into the statute. Under this proposal, government requests for the contents of communications as well as requests for expansive amounts of "noncontent" metadata would require a warrant and probable cause. Targeted and limited re-

* Law Clerk to the Honorable Joel Bolger, Alaska Supreme Court; J.D., Stanford Law School, 2014. I would like to thank Stacy Villalobos and her colleagues at the *Stanford Law Review* for shepherding this Note through its final stages, Robert Weisberg and George Fisher for their assistance at various points along the way, and Valerie Ong for her constant support and endless patience.

quests for noncontent data, however, would remain governed by the Stored Communications Act's current requirements. These changes would address the concerns articulated by the mosaic theory while improving the statute's ability to address future technological change.

INTRODUCTION

In *United States v. Jones*,[1] the Supreme Court relied on "18th-century tort law"[2] to dodge a decidedly twenty-first-century issue: Should Fourth Amendment doctrine account for the government's increasing technological ability to easily and inexpensively monitor suspects? And if so, how? The D.C. Circuit, in the case below, addressed the issue by introducing (or, more accurately, repurposing[3]) a novel approach that has been termed the "mosaic theory."[4] Under the mosaic theory, certain forms of long-term surveillance violate a suspect's reasonable expectation of privacy, even when each individual act of surveillance would itself pass Fourth Amendment muster, because the government can use the *aggregate* surveillance data to infer private details about the

1. 132 S. Ct. 945 (2012).

2. *Id.* at 957 (Alito, J., concurring in the judgment). Justice Scalia, writing for the majority, dismissed this characterization as a "distortion." *Id.* at 953 (majority opinion).

3. *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (drawing precedent from the government's deployment of the "mosaic theory" in national security cases), *aff'd on other grounds sub nom. Jones*, 132 S. Ct. 945.

4. *Id.* at 562; *see id.* at 560 ("[T]he whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil.").

suspect that no individual member of the public could reasonably learn by observing the suspect for a short time. Applying the mosaic theory, the D.C. Circuit held that the government's month-long, warrantless GPS surveillance of the defendant, Antoine Jones, violated his Fourth Amendment right to be free from unreasonable searches.[5] On appeal, the Supreme Court agreed that the police officers' behavior was unconstitutional but reached its holding on different grounds. Instead of addressing the month-long monitoring of Jones's movements, the majority focused on the police officers' warrantless installation of a physical GPS device on Jones's car, determining that even this de minimis physical trespass violated the Fourth Amendment.[6] While the Court's holding was more limited than privacy rights supporters might have preferred,[7] five Justices seemed willing to adopt some version of the mosaic theory, if not in *Jones* then in a future case not involving physical trespass.[8]

Although *Jones* was limited to GPS tracking, mosaic theory concerns logically extend to a wide range of new technologies. GPS technology endangers privacy by allowing the government, at very little cost, to monitor the physical movements of a suspect and infer private details about the suspect's life unrelated to the investigation.[9] Other types of technological surveillance pose similar, if not greater, privacy risks. Edward Snowden's disclosures have demonstrated the breadth of the National Security Agency's electronic surveillance efforts, including certain forms of domestic surveillance.[10] On a smaller scale, similar techniques are now used in domestic criminal investigations. Even after *Riley v. California*,[11] which prohibited warrantless searches of mobile phones, local, state, and federal law enforcement officers retain the ability to monitor suspects' activities by requesting personal information from telephone and Internet service providers.[12] The largest of these companies, which include traditional telecoms such as Verizon and Internet service providers such as Google,

---

5. *Id.* at 568.

6. *Jones*, 132 S. Ct. at 949-53.

7. *See, e.g.*, Rebecca J. Rosen, *Why the* Jones *Supreme Court Ruling on GPS Tracking Is Worse than It Sounds*, ATLANTIC (Jan. 23, 2012, 2:47 PM ET), http://www.theatlantic.com/technology/archive/2012/01/why-the-jones-supreme-court-ruling-on-gps-tracking-is-worse-than-it-sounds/251838 ("Combined, Sotomayor's and Alito's concurrences give us a picture of the more dramatic revisions to our Fourth Amendment understanding that would be required to protect privacy in our time. Scalia's opinion doesn't get there but, at least, in its narrowness, it doesn't take us in the wrong direction either.").

8. *See Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring in the judgment).

9. *Id.* at 955-56 (Sotomayor, J., concurring).

10. *See, e.g.*, Charlie Savage, *In Test Project, N.S.A. Tracked Cellphone Locations*, N.Y. TIMES (Oct. 2, 2013), http://www.nytimes.com/2013/10/03/us/nsa-experiment-traced-us-cellphone-locations.html (describing the ability to track cell phone locations and use "contact chaining" to analyze social networks).

11. 134 S. Ct. 2473 (2014).

12. Indeed, the *Riley* Court explicitly limited its holding to the search of mobile phone contents, not the collection and aggregation of the same data using other means. *Id.* at 2489 n.1.

often have access to users' Internet histories, search queries, e-mail correspondence, physical location information, and much more. And under the Stored Communications Act,[13] the government may require companies to disclose much of this information with only a court order or an administrative subpoena.[14] As a result of this compelled third-party assistance, the government can create a "mosaic" of users' online (and even offline) activities without being bound by the Fourth Amendment's typical warrant and probable cause requirements.

This Note argues that the Stored Communications Act's protections are inadequate in light of the conceptual insights of the mosaic theory and the massive technological changes that have occurred since the statute's passage in 1986. Part I explores the mosaic theory in more depth by analyzing the mosaic theory opinions in *Jones* and *United States v. Maynard*[15] (the case below). Part II documents modern companies' data collection capabilities to demonstrate why the current version of the Stored Communications Act fails to adequately protect Internet users' privacy. Part III proposes an amendment to the Stored Communications Act that incorporates a version of the mosaic theory.

I. DEFINING THE MOSAIC THEORY: *MAYNARD* AND *JONES*

Although the mosaic theory is conceptually broad enough to inform privacy policy in a wide range of technological contexts, the theory traces its origins to the government's use of a GPS tracking device in a fairly straightforward police investigation of a cocaine distribution conspiracy. In order to clarify the reasoning behind the theory before arguing for its integration into the Stored Communications Act, this Part summarizes the facts of the case, the D.C. Circuit's initial conception of the mosaic theory in *Maynard*, and the concurring Supreme Court Justices' slightly different definitions of the theory in *Jones*.

A. United States v. Maynard*: Introducing the Mosaic Theory*

In 2004, a joint FBI and Metropolitan Police Department task force began investigating Antoine Jones, a Washington, D.C., nightclub owner suspected of—and later charged with—conspiring to distribute drugs.[16] In 2005, the task

13. 18 U.S.C. §§ 2701-2712 (2013). The Stored Communications Act is a component of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2522, 2701-2712, 3121-3127).

14. 18 U.S.C. § 2703.

15. 615 F.3d 544 (D.C. Cir. 2010), *aff'd on other grounds sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

16. *Jones*, 132 S. Ct. at 948. At trial, Jones had a number of codefendants, including Lawrence Maynard, Jones's coappellant before the D.C. Circuit. *Maynard*, 615 F.3d at 549. Because Jones alone raised the GPS issue on appeal, the D.C. Circuit upheld Maynard's conviction, *id.* at 555, 568, and this Note summarizes only facts pertaining to Jones.

force applied for a warrant to place a GPS device on Jones's car.[17] Despite the officers' good faith efforts in *seeking* the warrant, they failed to follow the warrant's requirements.[18] The warrant granted the officers ten days to plant the device, but they did not do so until the eleventh.[19] The warrant also required them to install the device while Jones's car was parked in the District of Columbia, but they did so in Maryland.[20]

Over the next twenty-eight days, the device tracked the movements of Jones's car.[21] It relayed the car's location to the officers, who collected over 2000 pages of location data.[22] The officers relied on these data (combined with other evidence) to connect Jones to the conspiracy's stash house, which contained "$850,000 in cash, 97 kilograms of cocaine, and 1 kilogram of cocaine base."[23] At trial, Jones unsuccessfully attempted to suppress the GPS data, arguing that the officers violated the warrant requirements and lacked probable cause to suspect that his vehicle was connected to criminal activity.[24]

Relying on strikingly novel reasoning, the D.C. Circuit reversed, holding that "the extended recordation of a person's movements" without a proper warrant is outside the realm of reasonable searches.[25] To reach this conclusion, the appellate court borrowed the concept of the "mosaic theory" from national security cases.[26] In Freedom of Information Act cases, for example, intelligence agencies invoke the theory to defend against requests for disclosure, arguing that official disclosure of "superficially innocuous information" might allow "[f]oreign intelligence services . . . to . . . deduc[e] the identities of intelligence sources" merely from "knowing what is being studied and researched by [American] agencies."[27] The fear is that "[t]housands of bits and pieces of seemingly innocuous information can be analyzed and fitted into place to reveal with startling clarity how the unseen whole must operate."[28]

Transferring this reasoning to the criminal investigations context, the D.C. Circuit concluded that prolonged surveillance reveals not only additional information about a suspect but also information of a different kind,[29] the core insight of the mosaic theory. By monitoring an individual over a long period,

17. *Jones*, 132 S. Ct. at 948.

18. *Id.* at 948 & n.1.

19. *Id.* at 948.

20. *Id.* In fact, the agents later *reinstalled* the device on Jones's car during the surveillance period to replace the battery; once again, they did so in Maryland. *Id.*

21. *Id.*

22. *Id.*

23. *Id.* at 948-49.

24. United States v. Jones, 451 F. Supp. 2d 71, 87-88 (D.D.C. 2006), *rev'd sub nom.* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd on other grounds sub nom. Jones*, 132 S. Ct. 945.

25. *Maynard*, 615 F.3d at 562-64.

26. *Id.* at 562.

27. CIA v. Sims, 471 U.S. 159, 178 (1985).

28. Halkin v. Helms, 598 F.2d 1, 8 (D.C. Cir. 1978).

29. *Maynard*, 615 F.3d at 562.

the government can learn "whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts."[30] The appellate court then applied the mosaic theory in conjunction with the two-part *Katz* test, which requires defendants to demonstrate that their expectations of privacy are both subjectively held and objectively reasonable.[31] Under this test, the D.C. Circuit held that "Jones's [subjective] expectation of privacy in his movements over the course of a month" was one "[s]ociety recognizes . . . as reasonable."[32]

B. United States v. Jones *and* Riley v. California*: Complicating the Mosaic Theory*

The Supreme Court affirmed the D.C. Circuit's judgment on much narrower grounds. While Justice Scalia, writing for the majority, ruled in Jones's favor, he was unwilling to "rush[] forward to resolve" the issues the D.C. Circuit had raised below.[33] Instead of deciding whether the government's *prolonged surveillance* of Jones constituted an unreasonable search, the majority focused on a preliminary issue the D.C. Circuit had noted only in passing[34]: the *physical installation* of the GPS device on Jones's vehicle.[35] Citing the Fourth Amendment's historical purpose of protecting property, Justice Scalia concluded that the physical placement of a GPS device onto a car "constitutes a 'search'" warranting full Fourth Amendment protection.[36]

While the majority opinion did not adopt or reject the mosaic theory,[37] five Justices (including Justice Sotomayor, who also joined the majority) signaled their approval for some version of the D.C. Circuit's mosaic theory reasoning. Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, concurred in the

---

30. *Id.*

31. *Id.* at 563; *see* United States v. Katz, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[T]here 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.'").

32. *Maynard*, 615 F.3d at 563. To support this conclusion, the appellate court cited laws in eight states prohibiting GPS tracking without a warrant, finding them "indicative" of society's expectations of privacy. *Id.* at 564. The states were California, Florida, Hawaii, Minnesota, Oklahoma, Pennsylvania, South Carolina, and Utah. *Id.*

33. United States v. Jones, 132 S. Ct. 945, 954 (2012).

34. *Maynard*, 615 F.3d at 557.

35. *Jones*, 132 S. Ct. at 949-53.

36. *Id.* at 949-50.

37. Because the Supreme Court did not reverse *Maynard*, the case appears to remain good law in the D.C. Circuit. *See* Orin Kerr, *My Instincts Were Wrong—at Least I Now Think They Were—on* Maynard, VOLOKH CONSPIRACY (Dec. 3, 2013, 8:28 PM), http://www.volokh.com/2013/12/03/instincts-wrong-least-now-think-maynard. Indeed, in *Klayman v. Obama*, District Court Judge Leon cited *Maynard* as well as the *Jones* concurrences without questioning whether *Maynard*'s mosaic theory holding continued to bind trial courts in the D.C. Circuit. 957 F. Supp. 2d 1, 31, 36 (D.D.C. 2013).

judgment only, criticizing the majority's trespass-based reasoning and embracing the D.C. Circuit's mosaic theory.[38] Justice Sotomayor's separate concurrence announced her approval for the majority's narrow holding, while signaling her support for the mosaic theory as well as other significant changes to Fourth Amendment doctrine.[39] Unfortunately, while both concurring opinions built off of the D.C. Circuit's reasoning, they each tweaked the contours of the theory, making it more difficult to cleanly define.

Justice Alito's concurrence argued that the Court should integrate the mosaic theory into the existing *Katz* test,[40] as the D.C. Circuit had done in *Maynard*. Though his justification for the theory was quite brief and conclusory,[41] he clearly relied on the lower court's arguments in concluding that "relatively short-term monitoring of a person's movements . . . accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[42] Justice Alito did not, however, explicitly name the "mosaic theory" or cite *any* legal precedent (or even secondary sources) to support its adoption.[43] And like the decision in the court below, he left the details of the mosaic theory relatively undeveloped. He did not "identify with precision the point at which the tracking of [Jones's] vehicle became a search," stating merely that the line had been crossed at some point during the twenty-eight days of surveillance.[44] Moreover, Justice Alito declined to elaborate on how the theory would interact with other areas of Fourth Amendment doctrine, such as exigency, inevitable discovery, or the fruit of the poisonous tree.[45] If anything, his conception of the mosaic theory was more limited than the D.C. Circuit's. While the lower court seemed open to extending the theory beyond GPS surveillance—perhaps even to nontechnological, visual surveillance[46]—Justice Alito suggested that citizens' expectations of privacy might be reduced in the digital realm.[47]

---

38. *Jones*, 132 S. Ct. at 961, 964 (Alito, J., concurring in the judgment).

39. *Id.* at 954-57 (Sotomayor, J., concurring).

40. *Id.* at 959-60, 963-64 (Alito, J., concurring in the judgment).

41. *See id.* at 964.

42. *Id.* (citation omitted).

43. *See id.* at 963-64.

44. *Id.* at 964.

45. *See id.* ("Other cases may present more difficult questions.").

46. *See* United States v. Maynard, 615 F.3d 544, 566 (D.C. Cir. 2010), *aff'd on other grounds sub nom. Jones*, 132 S. Ct. 945.

47. *Jones*, 132 S. Ct. at 962 (Alito, J., concurring in the judgment) ("New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile."). *Riley* suggests there would be majority support on the Court for a broadly construed mosaic theory even if Justice Alito is unwilling to extend the theory beyond the GPS context. Chief Justice Roberts cited and largely echoed Justice Sotomayor's mosaic theory reasoning in his discussion of cell phone records, and his opinion was joined in full by all Justices except Justice Alito. *See infra* text accompanying notes 59-65.

In contrast, Justice Sotomayor's defense of the mosaic theory was more detailed and its potential reach more expansive. While she concluded that the majority's trespass-based reasoning sufficiently resolved the case,[48] she, like Justice Alito, recognized that the majority's limited holding would not adequately protect individuals against technological threats to privacy in future cases.[49] Justice Sotomayor's opinion, however, contemplated even more significant changes to Fourth Amendment doctrine, including not only the adoption of the mosaic theory but also the repeal of the third-party doctrine.[50]

Justice Sotomayor offered a full-throated defense of the mosaic theory that differed from those of Justice Alito and the D.C. Circuit.[51] While she shared Justice Alito's concern that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy," she appeared willing to apply the mosaic theory to even *short-term* surveillance, at least when GPS technology is used.[52] Even in such cases, she argued, "unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention" because "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[53] In other words, Justice Sotomayor seemed interested in measuring the creation of a mosaic not by the *temporal* length of the surveillance (as both Justice Alito and the D.C. Circuit suggested) but by the *quantity and quality* of the information collected. Regardless of the appropriate metric, however, Justice Sotomayor feared the ubiquity and low cost of GPS technology would allow the government to "store such records and efficiently mine them for information years into the future," "chill[ing] associational and expressive freedoms" if citizens fear their movements can be tracked and analyzed at will.[54]

Relatedly—and importantly, for reasons discussed below—Justice Sotomayor also questioned the ongoing suitability of the third-party doctrine in the Internet era: "[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[55] The third-party doctrine, she noted, allows the government to access phone numbers, e-mail addresses, Internet histories, and online shopping lists without a warrant.[56] Few people, Justice Sotomayor ar-

48. *Jones*, 132 S. Ct. at 954 (Sotomayor, J., concurring).

49. *Id.* at 955.

50. *Id.* at 957.

51. *Id.* at 955-56.

52. *Id.* at 955 (quoting *id.* at 964 (Alito, J., concurring in the judgment)) (internal quotation marks omitted).

53. *Id.*

54. *Id.* at 955-56.

55. *Id.* at 957.

56. *Id.* Had the government received Jones's GPS data through a third-party source such as OnStar, the third-party doctrine absent the mosaic theory (or the limited protections

gued, "would accept without complaint the warrantless disclosure to the Government" of such information.[57] While her discussion of the third-party doctrine was relatively brief, it demonstrated Justice Sotomayor's awareness that the mosaic theory could apply to technologies other than GPS devices.

Nevertheless, Justice Sotomayor's concurrence—like Justice Alito's—left the contours of the mosaic theory largely ambiguous.[58] She did not take a firm position on how much information the government may collect before it forms a mosaic. While suggesting that GPS surveillance poses acute privacy concerns not present in older technologies, she did not clarify which other new technologies pose similar concerns that might likewise suggest the immediate creation of a mosaic. And she did not conclusively indicate whether the theory should apply beyond the context of GPS surveillance or whether her proposed revisiting of the third-party doctrine would adequately address her privacy concerns.

But despite these omissions, Justice Sotomayor appears to have convinced the entire Court to take her concerns about digital privacy seriously. Two years later, in *Riley v. California*, the Court *unanimously* held that the Fourth Amendment prohibits warrantless searches of mobile phone contents.[59] While Chief Justice Roberts's opinion avoided ruling directly on the mosaic theory,[60] he nonetheless leaned heavily on its reasoning.[61] Observing the changing technological landscape, Chief Justice Roberts highlighted that "many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives."[62] And, citing Justice Sotomayor's *Jones* concurrence, he concluded that much of the data Americans carry around with them isn't merely "distinguished from physical records by quantity alone" but is "qualitatively different."[63] Channeling Justice Sotomayor—and the D.C. Circuit before her—Chief Justice Roberts noted that this information can provide the government with insights into citizens' health care choices, physical locations, political affiliations, substance addictions, relationship statuses, and so on.[64] Moreover, these individual insights may be combined into a "revealing montage"—read: mosaic—of citizens' lives.[65]

Because neither *Jones* nor *Riley* adopted the mosaic theory, however, Court watchers are left with three separate versions of the theory (the D.C. Circuit's,

---

of the Stored Communications Act) would have allowed the government to track Jones's movements indefinitely. *See id.*

57. *Id.*

58. *See id.* at 955-56.

59. 134 S. Ct. 2473, 2494-95 (2014). Chief Justice Roberts wrote the majority opinion, which Justices Scalia, Kennedy, Thomas, Ginsburg, Breyer, Sotomayor, and Kagan joined. *Id.* at 2479. Justice Alito authored a separate opinion, concurring in part and concurring in the judgment. *Id.* at 2495 (Alito, J., concurring in part and concurring in the judgment).

60. *See id.* at 2489 n.1 (majority opinion).

61. *See id.* at 2490-91.

62. *Id.* at 2490.

63. *Id.*

64. *Id.*

65. *Id.*

Justice Alito's, and Justice Sotomayor's), none of which is particularly fleshed out. But though these three conceptions of the theory differ in both minor and significant ways, they share the core insight that certain types of long-term (or otherwise extensive) surveillance pose acute threats to individuals' privacy. By collecting, aggregating, and analyzing information from such surveillance, the government may infer private details about a suspect that no individual member of the public could reasonably learn through more limited observation. This insight drives the discussion of online data collection methods in Part II and informs the proposed amendments to the Stored Communications Act in Part III.

II. ONLINE PRIVACY AND CURRENT LAW

While the pro-mosaic-theory opinions in *Maynard* and *Jones* (and, to a lesser extent, *Riley*) succeeded in explaining the privacy concerns inherent in the government's ability to collect and analyze extensive amounts of GPS data, they failed to clarify how the theory should be applied and to which technologies (other than GPS). These are important questions, especially in light of "cloud computing," which the Court has defined as "the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself."[66] Americans increasingly communicate and store their personal documents in the cloud, and the data that cloud computing collects and generates can be far more revealing than the location data GPS devices record.

This Part demonstrates the ability of telephone and Internet service providers to collect and store vast quantities of information, sufficient to construct detailed mosaics about their customers. It then explains why the Stored Communications Act,[67] which regulates the government's ability to request these data, is outdated and insufficient to protect Internet users' privacy.

A. *Telephone and Internet Data Collection*

Americans are increasingly leaving a "big data" trail. As Daniel J. Solove noted more than a decade ago:

> [L]ife in modern society demands that we enter into numerous relationships with professionals (doctors, lawyers, accountants), businesses (restaurants, video rental stores), merchants (bookstores, mail catalog companies), publishing companies (magazines, newspapers), organizations (charities), financial institutions (banks, investment firms, credit card companies), landlords, employers, and other entities (insurance companies, security companies, travel

66. *Id.* at 2491; *see also* Eric Griffith, *What Is Cloud Computing?*, PC MAG. (Mar. 13, 2013), http://www.pcmag.com/article2/0,2817,2372163,00.asp. Web-based e-mail services such as Gmail and Yahoo! Mail are cloud computing services, as are storage services such as Google Drive and Dropbox. Other examples include social networking websites such as Facebook and office productivity services such as Google Docs and Microsoft Office Online. *See id.*

67. 18 U.S.C. §§ 2701-2712 (2013).

> agencies, car rental companies, hotels). Our relationships with all of these entities generate records containing personal information necessary to establish an account and record of our transactions, preferences, purchases, and activities. We are becoming a society of records, and these records are not held by us, but by third parties.[68]

In the years since, this record-keeping has only intensified. Moreover, while Solove discussed a "series of records" held by a range of third parties,[69] the business strategies of many major Internet service providers, most notably Google, depend on acquiring as much information as possible about their customers from multiple sources and combining these data into centralized records, which these companies can use for a variety of purposes, including targeted advertising.[70] Because of this trend, our society is entering an era in which the government can uncover more information about an individual from a *single* information request to an Internet service provider than it could in 2002 via numerous requests to multiple third parties.

Even phone records, which the government can obtain from third parties by mere subpoena,[71] provide significant windows into the personal lives of mobile phone users. A simple study conducted by two Stanford University researchers in 2014 showed that the analysis of cell phone metadata—"noncontent" data that include the initiator and recipient of a call, the time of the call, and its duration—often reveals intimate personal details about the phone owners.[72] Using only these metadata and public websites such as Google and Yelp, the researchers could determine which phone owners contacted "sensitive organization[s]" such as health services, legal services, religious bodies, firearm sales and repair providers, adult establishments, and marijuana dispensaries.[73] In several cases, the researchers could infer even more sensitive information from the phones' metadata, including two individuals' medical conditions (relapsing multiple sclerosis in one case, cardiac arrhythmia in another), another person's attempt to purchase an AR semiautomatic rifle, and possibly a pregnant woman's inquiries into having an abortion.[74]

But while phone records such as these can reveal very private information, even *basic* Internet activities such as reading e-mail and browsing the web cre-

---

68. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1089 (2002).

69. *Id.* at 1090.

70. *See How Ads Are Targeted to Your Site*, GOOGLE, https://support.google.com/adsense/answer/9713?hl=en (last visited Feb. 23, 2015) ("Interest-based advertising enables advertisers to reach users based on their interests and demographics (e.g. 'sports enthusiasts'), and allows them to show ads based on a user's previous interactions with them, such as visits to advertiser websites.").

71. 18 U.S.C. § 2703(c)(1)-(2).

72. Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata*, WEB POL'Y (Mar. 12, 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata.

73. *Id.*

74. *Id.*

ate expansive metadata records that may reveal exponentially more. E-mail metadata records include, at a minimum, information about each message's sender and recipient, its subject line, and its date and time.[75] Likewise, Internet service providers keep records of the IP addresses their users access. These unique addresses—numbers assigned to devices and servers—allow online communications to be directed from the correct source to the proper destination and are therefore necessary for the Internet to function.[76] But they can reveal to the Internet service provider (or the government) not only the source of the information but also its content.[77] And online tracking services (which are invisible to Internet users and employed widely by advertising companies such as Google[78]) can record how long users stay on a webpage, which hyperlinks they click, and even where they place their cursor.[79]

Moreover, Internet companies' metadata collection is rapidly expanding as Internet users rely more and more heavily on mobile devices and cloud-based platforms, such as Google's myriad web services, Apple's iCloud, and Microsoft's Office Online service. When mobile phone users open their Google Maps or Facebook apps, their locations are typically sent to Google or Facebook.[80] Mobile app stores such as Apple's iTunes Store and Google's Play Store keep track of which apps users purchase and when.[81] Online storage platforms such as Dropbox, Google Drive, and Microsoft OneDrive store metadata

75. *A Guardian Guide to Your Metadata*, GUARDIAN (June 12, 2013, 11:52 AM EDT), http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance.

76. *What Is an IP Address?*, WHATISMYIPADDRESS.COM, http://whatismyipaddress.com/ip-address (last visited Feb. 23, 2015).

77. For example, the service provider or government can type users' IP address histories into a web caching service such as the "Wayback Machine" to view the contents of websites as they appeared when the users visited them. *See* INTERNET ARCHIVE, https://archive.org (last visited Feb. 23, 2015).

78. *About Google Ads*, GOOGLE, https://support.google.com/ads/answer/1634057 (last visited Feb. 23, 2015).

79. *About In-Page Analytics*, GOOGLE, https://support.google.com/analytics/answer/2558811 (last visited Feb. 23, 2015); Steve Rosenbush, *Facebook Tests Software to Track Your Cursor on Screen*, WALL ST. J. CIO REP. (Oct. 30, 2013, 7:15 AM ET), http://blogs.wsj.com/cio/2013/10/30/facebook-considers-vast-increase-in-data-collection.

80. *See* J.D. Biersdorfer, *Q&A: When Facebook Marks Your Spot*, N.Y. TIMES GADGETWISE (Feb. 13, 2012, 5:35 PM), http://gadgetwise.blogs.nytimes.com/2012/02/13/qa-when-facebook-marks-your-spot; Miguel Helft, *Google Says It Collects Location Data on Phones for Location Services*, N.Y. TIMES BITS (Apr. 22, 2011, 5:48 PM), http://bits.blogs.nytimes.com/2011/04/22/google-says-it-collects-location-data-on-phones-for-location-services. The user's consent is typically required the first time she opens one of these apps. *See Understanding Privacy and Location Services on iPhone, iPad, and iPod Touch with iOS 8*, APPLE, http://support.apple.com/en-us/HT6338 (last modified Nov. 14, 2014).

81. *See, e.g.*, *See Your Purchase History in the iTunes Store*, APPLE, http://support.apple.com/en-us/HT204088 (last modified Dec. 22, 2014).

that may contain labels, attachments, icons, information about which users have access to which files, and so on.[82]

Maintaining users' metadata allows Internet service providers to provide the functionalities their customers desire.[83] But Internet service providers have additional incentives to collect these data, most notably to facilitate targeted advertising. Google, for instance, makes almost all of its money, including eighty-four percent of its 2013 revenues, from advertising.[84] As Internet users increase their reliance on online platforms and services, Internet service providers will have access to expanding amounts of data—and the financial incentive to collect as much of it as they can.

Perhaps the best example of Internet service providers' current ability to collect, aggregate, and analyze users' data into a useable "mosaic" is the Google Now service. Google Now sends Android and iPhone users personalized and relevant information about their schedules and surroundings.[85] Google provides this information by collecting and aggregating data from an array of Google services—Gmail, Calendar, Maps, Google+, Play, etc.—and monitoring users' physical locations using their phones' location-tracking services.[86]

For instance, if Google Now users receive flight itineraries via Gmail, the service will automatically send terminal and gate information, delay notifications, and electronic boarding passes to their phones.[87] The app can even monitor traffic conditions and remind users when they need to leave for the airport.[88] When travelers using the service touch down at their destinations, Google Now provides public and private transportation suggestions (and driving directions if the travelers have hotel booking confirmations in their Gmail accounts).[89] And if the service detects that the travelers are in a foreign country, it will even provide translation services and currency exchange-rate information.[90]

Google Now provides many other types of information as well. Based on location history, for instance, the service knows where users live and work, and

---

82. *See, e.g.*, *What Types of Files Can I Store or View on Dropbox?*, DROPBOX, https://www.dropbox.com/en/help/6 (last visited Feb. 23, 2015).

83. For example, Google could not send Gmail messages if it did not know where to direct them.

84. *2013 Financial Tables*, GOOGLE INVESTOR REL., http://investor.google.com/financial/2013/tables.html (last visited Feb. 23, 2015).

85. Roy Furchgott, *How to Tell Google Now to Stop Peeking*, N.Y. TIMES GADGETWISE (May 7, 2013, 1:07 PM), http://gadgetwise.blogs.nytimes.com/2013/05/07/how-to-tell-google-now-to-stop-peeking.

86. *Id.*

87. *See See All the Cards*, GOOGLE, http://www.google.com/landing/now/#cards (last visited Feb. 23, 2015).

88. *See id.*

89. *See id.*

90. *See id*.

the app may suggest driving to work early if traffic is bad.[91] It provides reminders about appointments, restaurant reservations, and other events without users needing to actively request them.[92] It tracks the delivery of FedEx and UPS packages.[93] And it lists bus and train arrival times when it determines that a user is waiting at a public transit stop.[94]

Google Now's functionality will only increase in the future, and Google's competitors are rushing to provide similar services.[95] Some of these competitors are beginning to introduce wearable devices that collect entirely new types of information, including biometric data. For example, Fitbit sells devices that track their users' exercise regimens and sleep patterns.[96] And Apple, one of Google's primary competitors, will release its long-rumored Apple Watch in early 2015.[97] This "smart watch" will feature biometric sensors similar to Fitbit's as well as a heart rate monitor.[98] If these products are commercially successful, Google will likely add similar functionality to its competing Android Wear platform.

No doubt these expanding Internet services and mobile technologies are useful to consumers. But Google Now and competing services also demonstrate just how much information Internet service providers can now collect from their users. Analyzed in the aggregate, these data can reveal sensitive information about users' lives, both online and offline. In a pre-Internet world, much of this information would have been considered "private" under the Fourth Amendment, and no *single* company would have dreamed of having access to all of it.

---

91. Erica Ogg, *Siri, Watch Out: Personalized Search Service Google Now Is Coming to iOS*, GIGAOM (Apr. 29, 2013, 7:15 AM PDT), http://gigaom.com/2013/04/29/siri-watch-out-personalized-search-service-google-now-is-coming-to-ios.

92. *See See All the Cards*, *supra* note 87.

93. *Id.*

94. *Id.*

95. Apple responded to Google Now in 2013 by adding similar (if much more limited) functionality to the iPhone. Juli Clover, *Apple's Google Now Competitor 'Today' Features Traffic Information on Frequently Visited Locations*, MACRUMORS (June 12, 2013, 2:59 PM PDT), http://www.macrumors.com/2013/06/12/today-feature-in-notification-center-provides-traffic-information-for-frequently-visited-locations. In 2014, Microsoft introduced "Cortana" on its Windows Phone operating system, and the company will soon extend this service to Windows-based computers as well; Cortana provides functionality similar to both Apple's Siri and Google Now. Nate Ralph, *Cortana Jumps from Phone to Desktop with Windows 10 (Hands-On)*, CNET (Jan. 29, 2015, 5:00 PM PST), http://www.cnet.com/products/microsoft-cortana.

96. *Fitbit Tracker Comparison*, FITBIT, http://www.fitbit.com/compare (last visited Feb. 23, 2015).

97. *Apple Watch—Overview*, APPLE, http://www.apple.com/watch/overview (last visited Feb. 23, 2015).

98. *Apple Watch—Technology*, APPLE, http://www.apple.com/watch/technology (last visited Feb. 23, 2015).

B. *The Insufficient Protection of Online Privacy Under Current Law*

There is little constitutional protection for user data collected from these online services because the institutional third-party doctrine holds that information a customer voluntarily provides to a third party may be disclosed to the government without violating the Fourth Amendment.[99] Instead, most government requests for this information are governed by the Stored Communications Act,[100] a now-antiquated statute designed to protect users from the digital privacy threats of the 1980s. Yet a recent Sixth Circuit case, *United States v. Warshak*, has called the legitimacy of the third-party doctrine and the Stored Communications Act into question, at least regarding the contents of e-mails and other digital *communications* (but not metadata or other noncontent information).[101] This Subpart briefly discusses these developments.

1. *The third-party doctrine*

Since the late 1970s, the Supreme Court has held that the Fourth Amendment offers little, if any, protection to information individuals have shared with institutional third parties. This institutional third-party doctrine originated as a logical extension of the existing individual third-party doctrine, which primarily addresses disclosures made to police informants and undercover officers.[102] Nevertheless, the Court in 1979 could not have predicted the extent to which modern society would come to depend on third parties for basic communications and personal data storage. Indeed, the two cases that most clearly defined the institutional third-party doctrine involved paper documents,[103] microfilms,[104] and rotary telephones.[105]

In *United States v. Miller*, the Supreme Court held that criminal defendants lack a reasonable expectation of privacy in documents disclosed to institutional third parties "even if 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."[106]

---

99. Smith v. Maryland, 442 U.S. 735, 745-46 (1979); United States v. Miller, 425 U.S. 435, 440-43 (1976).

100. 18 U.S.C. §§ 2701-2712 (2013).

101. 631 F.3d 266, 282-88 (6th Cir. 2010).

102. *See* United States v. White, 401 U.S. 745, 751-52 (1971) (plurality opinion) (finding no constitutional distinction between a police agent taking notes about a conversation with the accused and recording or transmitting that conversation); Hoffa v. United States, 385 U.S. 293, 302 (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").

103. *Miller*, 425 U.S. at 442.

104. *Id.*

105. *See* Smith v. Maryland, 442 U.S. 735, 737 (1979).

106. *Miller*, 425 U.S. at 443.

In *Smith v. Maryland*, the Court extended the third-party doctrine to cover government requests for *prospective* information gathering (and subsequent disclosures to the government).[107] The technology used to collect the information was a "pen register," which recorded the telephone numbers dialed on a phone.[108] This device was installed by police request at the phone company's central office.[109] Applying *Katz*, the Court expressed doubt that telephone users "entertain any actual expectation of privacy in the numbers they dial," since they realize that they must share that information with the telephone company in order to initiate calls in the first place.[110] It was immaterial to the Court's analysis that the telephone company collected and stored this information only at the government's request.[111]

Justices Brennan and Marshall dissented in both cases. Justice Brennan argued that individuals retain an expectation of privacy in their bank statements and records.[112] And Justice Marshall criticized the Court's binary view of privacy. Even if telephone users expected phone companies to keep track of telephone numbers for "internal reasons," he argued,

> it does not follow that they expect this information to be made available to the public in general or the government in particular. *Privacy is not a discrete commodity, possessed absolutely or not at all.* Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.[113]

Moreover, Justice Marshall argued, individuals who wish to participate in modern society have little choice but to disclose information to companies such as banks and telephone service providers.[114]

Justice Stewart also dissented in *Smith*, arguing that telephone numbers "are not without 'content.'"[115] He doubted anyone "would be happy to have broadcast to the world a list of the local or long distance numbers they have called."[116] Telegraphing the argument that would later underlie the mosaic theory, he reasoned, "This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[117]

---

107. *Smith*, 442 U.S. at 737, 745-46.

108. *Id.* at 736 n.1.

109. *Id.* at 737.

110. *Id.* at 742.

111. *See id.* at 737 ("[T]he telephone company, at police request, installed a pen register at its central offices to record the numbers dialed from the telephone at petitioner's home.").

112. United States v. Miller, 425 U.S. 435, 448 (1976) (Brennan, J., dissenting).

113. *Smith*, 442 U.S. at 749 (Marshall, J., dissenting) (emphasis added).

114. *Id.* at 749-50.

115. *Id.* at 748 (Stewart, J., dissenting).

116. *Id.*

117. *Id.*

The rise of "big data" has vindicated the dissenting Justices' criticisms of the *Miller* and *Smith* holdings. Yet even before the Internet age, Congress acted to address these new privacy threats, though the legislation it passed focused on then-existing technologies and has failed to adapt to the modern era.

2. *The Electronic Communications Privacy Act*

Responding primarily to the need to address digital wiretapping "in light of dramatic changes in new computer and telecommunications technologies,"[118] Congress passed the Electronic Communications Privacy Act in 1986.[119] Title I of this legislation extended standard wiretap protections to electronic communications while in transit. Title II (also called the Stored Communications Act) provided protections for electronic communications stored by third parties, limiting *Miller*'s practical reach. And Title III regulated the use of pen registers, partially addressing Justice Marshall's concerns in *Smith*.

The Stored Communications Act[120] is the most relevant portion of the Electronic Communications Privacy Act for this Note. It criminalizes unauthorized access to users' stored communications,[121] restricts Internet service providers from voluntarily sharing those communications,[122] and regulates the government's ability to request user data from those providers.[123] As a result, government requests for the types of data discussed above in Part II.A are governed by the Stored Communications Act.

The passage of the Stored Communications Act—which occurred at a time when few citizens owned personal computers,[124] let alone had access to outside networks—was remarkably forward looking. But even those on the cutting edge of technology in the 1980s could never have predicted the ways in which human communications (and the technologies facilitating them) would evolve over the following decades. As a result, an effective shield against Reagan-era privacy concerns has gaping statutory holes in its protection against modern privacy threats.

There are five main problems with the Stored Communications Act, which are discussed in more detail below. First, it is based on a 1980s conception of technology and does not sufficiently guard against government requests for both content and noncontent data in the modern context. Second, and relatedly, the law's terminology is outdated, which makes the boundaries of its protec-

---

118. 132 CONG. REC. 14,608 (1986).

119. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2522, 2701-2712, 3121-3127 (2013)).

120. 18 U.S.C. §§ 2701-2712.

121. *Id.* § 2701.

122. *Id.* § 2702.

123. *Id.* § 2703.

124. In 1987, "only 15% of American homes ha[d] a computer—and the other 85% d[id]n't seem the least bit interested." Dan Gutman, *What Happened to the Computer Revolution?*, COMMODORE MAG., Sept. 1987, at 50, 50.

tions unclear. Third, it lacks a suppression remedy, so information obtained in violation of the law may still be admitted against criminal defendants. Because defendants have little incentive to raise the law as a result, courts have had few opportunities to construe the law in the criminal investigations context. Fourth, *United States v. Warshak* suggests the law—at least its provisions governing the disclosure of e-mail contents—is unconstitutional.[125] And fifth, the law fails to account for the privacy concerns revealed by the mosaic theory.

Perhaps most importantly, the Stored Communications Act's tiered framework relies on outdated conceptions of technology that do not adequately protect even the *contents* of Internet communications. The Act grants the highest level of protection for unopened e-mails (and other electronic communications "in an electronic communications system") that have been in storage for 180 days or less.[126] To request access to such communications, the government must obtain a warrant backed by probable cause.[127] The Act provides the second-highest tier of protection for noncontent data (including most of the data discussed in Part II.A), which the government may request using either a warrant or a court order.[128] At the third tier, the government may request access to opened e-mails, unopened e-mails and other communications stored longer than 180 days, or communications in a "remote computing service" via a warrant (without notice to the user), a court order (with notice to the user), or an administrative subpoena (with notice to the user).[129] Finally, at the lowest tier, the government need only issue an administrative subpoena (without notice to the user) to request access to the subscriber's basic account information: the customer's name, address, telephone or IP number, telephone records, and payment information.[130]

This tiered scheme—which treats opened e-mails differently than unopened ones, and e-mails older than 180 days differently than newer ones—made some sense in the technological context of the 1980s. At the time, unopened e-mails were stored in electronic storage only until a user accessed her e-mail, at which time all incoming e-mails would be copied to her personal computer and deleted from the server.[131] Thus, opened e-mails generally were not stored on the third-party server, and unopened e-mails stored for longer than 180 days were arguably abandoned because the user had failed to check her e-mail for six months (and likely never would).

---

125. 631 F.3d 266, 288 (6th Cir. 2010).

126. 18 U.S.C. § 2703(a).

127. *See id.*; FED. R. CRIM. P. 41(d)(1).

128. 18 U.S.C. § 2703(c)(1).

129. *Id.* § 2703(a)-(b).

130. *Id.* § 2703(c)(2)-(3). The government can also obtain this account information using a court order or warrant. *Id.*

131. Eric Z. Goodnight, *Email: What's the Difference Between POP3, IMAP, and Exchange?*, HOW-TO GEEK (Sept. 29, 2014), http://www.howtogeek.com/99423/email-whats-the-difference-in-pop3-imap-and-exchange.

Modern e-mail technology works quite differently. Most e-mail users now access their messages using one of two methods, neither of which automatically deletes the opened message from the e-mail server. First, many e-mail users access their messages via their web browsers using Internet e-mail services such as Gmail. These services are run in the cloud, and the software that opens, sends, and archives the communications is maintained on third-party servers, not users' computers.[132] Second, e-mail users who use local software to download messages to their personal computers or mobile devices typically "sync" their various devices with their remote e-mail provider.[133] Doing so allows users to maintain complete records of the e-mail on all of their devices, but it requires them to store their complete e-mail histories on the third party's servers. From a usage standpoint, both new approaches are superior to the old method of downloading messages to a single device. From a legal standpoint, however, these newer technologies open the door to privacy concerns because the communications remain in the hands of third parties. And under the Stored Communications Act, the government need only issue an *administrative subpoena*—not obtain a warrant or even a court order from a judge—to require the e-mail provider to turn over the contents of opened e-mails or e-mails that have remained unopened for 180 days.[134]

The Stored Communications Act's second major flaw is that its dated terminology threatens its effectiveness. The law protects only communications stored in an "electronic communications system" or a "remote computing service,"[135] and it provides only a cursory definition of what the latter term means.[136] Because Internet communications take on very different forms now than they did in the 1980s, the law's definitions risk being underinclusive (or even overinclusive) in ways its drafters could not have anticipated.[137]

Third, the Stored Communications Act's lack of a suppression remedy,[138] which would prevent the government from introducing information obtained in

---

132. *Id.*

133. *Id.*

134. 18 U.S.C. § 2703(a)-(b).

135. *Id.* § 2703.

136. The statute's definition of remote computing service is a "provision to the public of computer storage or processing services by means of an electronic communications system." *Id.* § 2711.

137. The Stored Communications Act's legislative history suggests that "processing services" referred specifically to "outsourcing functions," whereby companies would, for example, "send raw data to a remote computing service and ask the service to crunch numbers to calculate its payroll." 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, 1230 (2004). The outsourcing of such activities to remote servers became far less common as individuals and companies installed spreadsheet and database software on their own computers and internal servers. Ironically, however, cloud computing is making remote computing more common again and may revive this portion of the law. *See id.* at 1230-31 (discussing how eBay's online bidding calculations might be considered a remote computing service).

138. *See* 18 U.S.C. §§ 2701-2712 (containing no suppression remedy).

violation of the statute,[139] has prevented courts from clarifying the law's boundaries. Because criminal defendants cannot suppress evidence the government has obtained through a violation (or potential violation) of the Stored Communications Act, they have little incentive to challenge disclosures of their data. As a result, little case law construes the Stored Communications Act in the criminal context.[140]

Fourth, the portion of the Stored Communications Act allowing the government to request the contents of online communications without a warrant[141] is likely unconstitutional. In 2010, the Sixth Circuit held in *United States v. Warshak* that an e-mail "subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP.'"[142] Over Warshak's objection at trial, the court had allowed the government to introduce into evidence the contents of his e-mails, which demonstrated the fraudulent nature of his herbal supplement and penis enlargement business.[143] On appeal, he argued that the Fourth Amendment compelled the government to obtain a warrant before seeking the contents of his e-mails, notwithstanding the Stored Communications Act's more lenient standard.[144] And the appellate court agreed that there was little justification for treating e-mails differently than letters and telephone conversations: "As some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise."[145] The Sixth Circuit found the Stored Communications Act unconstitutional "to the extent that the SCA purports to permit the government to obtain . . . emails warrantlessly" from commercial Internet service providers.[146] As a result of *Warshak*, many large Internet service providers now demand warrants before disclosing content information, even in other judicial circuits.[147]

Finally, the Stored Communications Act does not address any of the "big data" concerns underlying the mosaic theory. The law does not recognize that a myriad of individually insignificant data points can be just as revealing in the aggregate as a single revealing disclosure. It does not distinguish between government requests for a day's, a month's, a year's, or even a lifetime's worth of

---

139. *Cf. id.* § 2515 (requiring the suppression of evidence obtained through illegal telephone wiretaps).

140. Kerr, *supra* note 137, at 1241.

141. 18 U.S.C. § 2703(a)-(b).

142. 631 F.3d 266, 288 (6th Cir. 2010) (quoting Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007)).

143. *Id.* at 276, 281.

144. *Id.* at 282.

145. *Id.* at 285-86.

146. *Id.* at 288. The court nevertheless declined to suppress the e-mail evidence because the government had relied in good faith on the Stored Communications Act to authorize the search. *Id.* at 288-92.

147. NATE CARDOZO ET AL., ELEC. FRONTIER FOUND., WHO HAS YOUR BACK?: PROTECTING YOUR DATA FROM GOVERNMENT REQUESTS 13-14, 18 (2014), *available at* https://www.eff.org/files/2014/05/15/who-has-your-back-2014-govt-data-requests.pdf.

data. And it does not envision that third parties would ever amass as much information as they do about so many aspects of their customers' lives.

In short, the Stored Communications Act is an overly complex, confusing, and outdated tool for protecting citizens' privacy at a time when Americans need that protection more than ever. As *Warshak* demonstrates, courts are beginning to recognize that the law fails to sufficiently combat the threat the third-party doctrine poses to citizens' privacy. The concurring opinions in *Jones*—most notably Justice Sotomayor's—suggest that the Supreme Court may be reconsidering whether the third-party doctrine (on which the Stored Communications Act relies) remains appropriate. Change seems inevitable because the status quo is unstable. But whether that change is led by the Court or by Congress remains to be seen.

III. REFORMING THE STORED COMMUNICATIONS ACT

A constitutional holding by the Supreme Court adopting the mosaic theory might seem a satisfying solution to the practical and legal concerns demonstrated in Part II. But such an approach is unlikely to adequately address current privacy concerns, let alone those arising in the future. This Part argues that a statutory amendment to the Stored Communications Act would be preferable to a judicially crafted solution. Subpart A explains the problems with a judicial solution and discusses the benefits of statutory reform in this area. Subpart B proposes an amendment to the Stored Communications Act that would conform the law to *Warshak*'s holding as well as expand its protections for individuals' data, consistent with the mosaic theory opinions of the D.C. Circuit and the concurring Justices in *Jones*. And Subpart C compares this Note's proposal to two others: Orin Kerr's suggested changes to the statute and the Email Privacy Act, a House bill to amend the law.

A. *The Need for a Statutory Solution*

Fast-paced technological change has destabilized the current statutory and constitutional framework for protecting citizens' privacy. Simultaneously, it poses a challenge to courts wishing to craft appropriate, narrowly tailored solutions.

The last fundamental shift in Fourth Amendment doctrine—*Katz v. United States*[148]—occurred in the 1960s and was brought on by the ubiquity of landline telephones and fears about unchecked government wiretapping efforts. In deciding *Katz*, the Court addressed a largely static technological concern. Telephones were already a relatively old technology, and the Court had previously

148. 389 U.S. 347 (1967). *Katz* provided (in Justice Harlan's concurrence) the general two-part test that courts use to determine whether government searches violate the Fourth Amendment. *See supra* note 31 and accompanying text.

addressed wiretapping *four decades* earlier.[149] Moreover, traditional landline telephones would remain the primary mode of instant, long-distance communication for at least two decades to come. When the Court issued the *Katz* decision in 1967, it could be confident its holding would be sustainable over the long term.

In contrast, the last three decades have seen constant—and rapid—technological change. Telephones transitioned from landlines to mobile phones and later to smartphones, which allow for voice, e-mail, and web-based communications. E-mails, text messages, and other forms of instant messaging have largely replaced paper letters. Websites have evolved from static, text-based documents to multimedia experiences to interactive cloud software platforms. Many of these changes—most notably the rise of smartphones and other highly mobile computing devices—date only to the last decade. And there is little indication that the pace of technological change is slowing, that the "next big thing" is not waiting just around the corner.

In this fast-changing context, it is often better to formulate privacy law through legislation than by judicial holding, as Kerr has convincingly argued.[150] While philosophical justifications support this conclusion, this Note's primary interest is practical: unlike the courts, Congress can pass sweeping but intricate policy schemes to address present and future concerns, and legislation is not bound by stare decisis.

Courts must rule on a case-by-case basis, whereas Congress may anticipate a wide range of circumstances and enact carefully tailored legislation. The *Maynard* opinion and Justice Alito's concurrence in *Jones* provide good examples of courts' difficulties crafting all-encompassing regulatory schemes. The D.C. Circuit ruled that Jones's privacy had been violated at some point during the twenty-eight days of GPS surveillance.[151] Justice Alito agreed.[152] Neither opinion, however, attempted to determine with precision how long was too long. And neither opinion defined with any clarity the types and techniques of surveillance to which the mosaic theory applied. Congress, on the other hand, can address many or all of these questions in a single act.

Then, too, courts generally adjudicate *past* disputes, whereas Congress legislates *future* policy. As a result, judicial holdings regarding fast-changing subjects tend to be outdated on arrival, while legislation can address present and

149. *See* Olmstead v. United States, 277 U.S. 438 (1928).

150. *See generally* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004).

151. United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010) ("Application of the test in *Katz* and its sequellae to the facts of this case can lead to only one conclusion: Society recognizes Jones's expectation of privacy in his movements over the course of a month as reasonable . . . ."), *aff'd on other grounds sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

152. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.").

future concerns. The initial passage of the Electronic Communications Privacy Act of 1986, which (for all its faults) largely protected e-mail communications and other online interactions at a time when few Americans owned or used personal computers, is a testament to the lasting power of legislation.

Finally, courts are generally bound by precedent, while Congress is not. With the exception of the Supreme Court, most courts cannot make sweeping policy changes. Legislatures, on the other hand, can repeal, modify, or pass new policies; indeed, that is their primary purpose. While institutional and political forces often cause legislatures to support (or, by not acting, resort to) the status quo,[153] Congress remains better equipped than courts to plot out new policy directions.

Proponents of a judicial solution, such as Solove, argue that privacy legislation has been less comprehensive, less clear, and less adaptive to technological change than Fourth Amendment case law.[154] Solove notes that Congress has failed to regulate many technologies, including satellites, radio frequency identification devices, and thermal imaging devices.[155] He argues that privacy statutes are "just as unclear as the Fourth Amendment—perhaps even more so."[156] And, citing the Electronic Communications Privacy Act as well as the 1934 predecessor to the Wiretap Act, he suggests that Congress is not particularly adept at crafting privacy legislation when it does act.[157]

But these criticisms of legislative action are overstated or apply equally to judicial action. While it is not difficult to list areas in which Congress has failed to act (or to act comprehensively), one can just as easily point to technologies raising privacy concerns that *courts* have failed to regulate through the Fourth Amendment: aerial surveillance, chemical testing, and communications systems, to name a few.[158] And even when courts do act, they often do so decades late. *Jones* was decided seventeen years after the Global Positioning System went online in 1995.[159] *Warshak* was decided twenty-four years after Congress passed the Electronic Communications Privacy Act.[160] *Riley* was decided thirty-one years after the FCC approved the first mobile phone for commercial

153. *See* Ezra Klein, *14 Reasons Why This Is the Worst Congress Ever*, WASH. POST WONKBLOG (July 13, 2012), http://wapo.st/1BQs88D (describing the inaction of the 112th Congress).

154. DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 165-67 (2011).

155. *Id.* at 165.

156. *Id.* at 166.

157. *Id.* at 166-67.

158. *See* Kerr, *supra* note 150, at 828-30.

159. *See* United States v. Jones, 132 S. Ct. 945 (2012); *Frequently Asked Questions*, GPS.GOV, http://www.gps.gov/support/faq (last modified July 31, 2014).

160. *See* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2522, 2701-2712, 3121-3127 (2013)).

use.[161] And the third-party doctrine continues to prevent meaningful constitutional protection for users' documents kept in cloud storage.[162] Congress may not have the best record on proactively protecting citizens from technological threats to privacy, but neither do the courts.

Moreover, although Solove is correct that privacy statutes are often more complex than Fourth Amendment doctrine, the relative simplicity of courts' privacy solutions can present their own problems. Fourth Amendment doctrine is typically binary. Under the Fourth Amendment, courts generally either recognize a reasonable expectation of privacy or they do not. If courts find this reasonable expectation of privacy, the Fourth Amendment will require a warrant and probable cause; if not, the Constitution provides little or no protection. The bluntness of Fourth Amendment doctrine causes courts to hesitate before extending privacy protections to new areas,[163] and it narrows the range of policy solutions that courts may implement.[164] Congress, on the other hand, has many policy levers it may pull, including intermediate evidentiary showing requirements for police (for example, "reasonable suspicion" instead of "probable cause"),[165] notice requirements,[166] and civil remedies.[167] In regulating a technological issue such as metadata, where small amounts reveal little but large amounts reveal a great deal, gradations in protection are not only appropriate but preferable to courts' typical all-or-nothing approach to the Fourth Amendment.

---

161. *See* Riley v. California, 134 S. Ct. 2473 (2014); *About Motorola*, MOTOROLA, https://www.motorola.com/us/consumers/about-motorola-us/About_Motorola-History-Timeline/About_Motorola-History-Timeline.html (last visited Feb. 23, 2015).

162. *See supra* text accompanying notes 102-17.

163. *See* Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 542 (2013) (discussing courts' hesitation to acknowledge a *Katz* reasonable expectation of privacy in a "wide variety" of cases).

164. After oral argument in *Riley*, some Court watchers predicted that the Court would try to narrowly tailor its holding to allow cell phone searches in some cases but not others, perhaps allowing searches for serious offenses only or when police had reason to suspect evidence pertaining to the offense of arrest might be on the phone. *See* Amy Howe, *A Whole New World: Today's Oral Arguments in Plain English*, SCOTUSBLOG (Apr. 29, 2014, 5:20 PM), http://www.scotusblog.com/2014/04/a-whole-new-world-todays-oral-arguments-in-plain-english ("[E]ven if California and the federal government seem unlikely to win outright, the chances that the Court will require police officers to get a warrant whenever they want to search an arrestee's phone appear even slimmer."); Dahlia Lithwick, *Our Cellphones Are Us*, SLATE (Apr. 29, 2014, 6:59 PM), http://slate.me/1AYc0W3. But contrary to these predictions, the Court ended up using its normal approach when extending Fourth Amendment protections to a new area: finding a reasonable expectation of privacy, then requiring probable cause and a warrant. *Riley*, 134 S. Ct. at 2494-95.

165. *See* 18 U.S.C. § 2703(d).

166. *See id.* § 2703(b)(1)(B).

167. *See id.* § 2707.

Of course, there is little question that legislatures bring their own unique downsides to the policy process, such as special interest capture[168] and excessive partisan gridlock.[169] But there are reasons to believe these concerns are diminished in this area. Legislative capture should not prevent privacy-increasing reform because many of the relevant corporate parties, including Internet service providers, have a commercial interest in keeping the data they hold to themselves.[170] Customer data becomes less valuable when it is widely known and no longer exclusive,[171] and customers place more trust in companies they feel will protect their privacy and information.[172] As a result, regulating metadata privacy is a rare issue on which privacy activists and giant corporations can join forces, at least as far as regulating disclosures of user data to the government. And partisan gridlock is less rigid here than on other critical issues because privacy reforms attract political support from both the left and the libertarian right.[173]

Furthermore, though prosecution-minded politicians and government agencies will no doubt oppose reforms that increase the government's investigative burdens,[174] several countervailing forces make reform nonetheless possible. First, the last few years have seen a slow decline in the "tough on crime" movement, and key conservatives, including Newt Gingrich and Grover

168. *See* Patrick Luff, *Captured Legislatures and Public-Interested Courts*, 2013 UTAH L. REV. 519, 525-27 (describing public choice theory's concept of legislative capture).

169. *See* Michael J. Teter, *Congressional Gridlock's Threat to Separation of Powers*, 2013 WIS. L. REV. 1097, 1101-11 (arguing that Congress is currently gridlocked and that the Framers did not intend this outcome).

170. Indeed, many of the largest Internet service providers, including Apple, Google, and Microsoft, have actively lobbied to reform the Electronic Communications Privacy Act. CARDOZO ET AL., *supra* note 147, at 17-18.

171. In this way, the value of customer data may be compared to trade secrets in intellectual property law. *Cf.* UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 538 (2009) ("'Trade secret' means information . . . deriv[ing] independent economic value . . . from not being generally known to . . . other persons . . . .").

172. After Target's infamous 2013 credit card breach became public, the retailer's sales fell, even as the company introduced across-the-board discounts to lure back customers. Elizabeth A. Harris, *Data Breach Hurts Profit at Target*, N.Y. TIMES (Feb. 26, 2014), http://www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html.

173. Representative Justin Amash proposed a legislative amendment that would have defunded the National Security Agency's domestic telephone metadata collection program. The narrowly defeated amendment had significant bipartisan support. Austin Wright, *Justin Amash Prevails as Amendment Fails*, POLITICO (July 24, 2013, 7:27 PM EDT), http://www.politico.com/story/2013/07/justin-amash-nsa-amendment-94722.html. Likewise, a *majority* of House members cosponsored the Email Privacy Act, which would amend the Stored Communications Act to comply with *Warshak*. *See infra* note 210 and accompanying text.

174. *See, e.g.*, David Perera, *Opposition Mounts to Proposed Civil Investigation Exemption from ECPA Amendments Act*, FIERCEGOVERNMENTIT (July 31, 2013), http://www.fiercegovernmentit.com/story/opposition-mounts-proposed-civil-investigation-exemption-ecpa-amendments-ac/2013-07-31.

Norquist, have publicly advocated for criminal justice reform.[175] Coinciding with this trend, the number of prison admissions in state and federal facilities has dropped sharply over the last decade, from the all-time high of 747,031 in 2006 to 609,781 in 2012.[176] Second, media scrutiny over federal surveillance methods—triggered in large part by Edward Snowden's leaked disclosures about the National Security Agency's mass surveillance practices—has put pressure on Congress to act.[177] And third, judicial decisions such as *Warshak* are eroding the current statutory scheme and increasing that pressure.[178] None of these factors guarantee legislative action, but together they create an environment in which privacy reformers may be able to overcome the usual opponents of reform.

In this political environment, legislative reform of online privacy law is not only needed but possible.

B. *The Proposed Amendment to the Stored Communications Act*

The Stored Communications Act may be flawed, but it can be fixed. The following proposal demonstrates how the law could address mosaic theory concerns with only a few significant changes.[179] First, the proposed amendment modifies the statute's tiered framework to both incorporate a time-based mosaic cutoff for warrantless disclosures and make the statute easier to follow and apply. Second, the proposed amendment adds a suppression remedy for government violations of the law, bringing the statute's remedies into line with the Fourth Amendment's typical protections. Incorporating this suppression remedy will also ensure that the Stored Communications Act will be litigated in the criminal context, allowing courts to interpret and apply the statute to changing circumstances. Finally, the proposed amendment replaces the terms "electronic communication service" and "remote computing service" with "network service." This change would remove a somewhat artificial distinction in the mod-

175. *See* Marc Mauer, *Is the 'Tough on Crime' Movement on Its Way out?*, MSNBC (May 22, 2014, 8:01 PM), http://www.msnbc.com/msnbc/sentencing-reform-the-end-tough-crime.

176. E. ANN CARSON & DANIELA GOLINELLI, BUREAU OF JUSTICE STATISTICS, PRISONERS IN 2012: TRENDS IN ADMISSIONS AND RELEASES, 1991-2012, at 3 tbl.1 (2013).

177. *See* Darren Samuelsohn, *Hill Draws Criticism over NSA Oversight*, POLITICO (Mar. 2, 2014, 10:14 PM EST), http://www.politico.com/story/2014/03/hill-draws-criticism-over-nsa-oversight-104151.html.

178. *See supra* text accompanying notes 141-47.

179. This proposal would retain the other sections of the Stored Communications Act as they are or with minor revisions to reflect revised section numbering. But other proposals to amend the statute are compatible with this one. For instance, Christopher Slobogin has proposed including additional civil remedies to protect the privacy of nondefendants. Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y (SPECIAL ISSUE) 1, 34-35 (2012). Such a reform would improve the Stored Communications Act's ability to protect citizens' privacy without conflicting with this Note's proposal.

ern technological context, clarify that the Act should be interpreted broadly, and ensure its continued applicability to emerging technologies.[180]

1. *Incorporating a three-tiered mosaic framework*

This proposal's first, most significant change to the Stored Communications Act would reorganize and amend 18 U.S.C. § 2703, which regulates the government's ability to compel institutional third parties to disclose their customers' stored data. While the current version of the statute is effectively tiered in its protections, this amendment would make the tiers of protection simpler and more transparent. Subsection (a), the highest tier, would protect content data from disclosure without a warrant. Subsection (b), the intermediate tier, would incorporate the mosaic theory and protect against sweeping requests for metadata. Subsection (c), the lowest tier, would provide limited protections against less invasive disclosures. Each of these amended subsections is explained in more detail below.

The Revised Statute—18 U.S.C. § 2703(a)

> **(a) Contents of Wire or Electronic Communications ~~in Electronic Storage~~ or Documents Held by Network Service Providers.**—A governmental entity may require the disclosure by a network service provider of—
>
> > **(1)** ~~a provider of electronic communication service of~~ the nonpublic contents of a wire or electronic communication~~, that is in electronic storage in an electronic communications system for one hundred and eighty days or less~~; or
> >
> > **(2)** the nonpublic contents of any document held or maintained on that service on behalf of a subscriber of such service,
>
> only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. ~~A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.~~

180. In addition to the blacklined excerpts of this Note's proposed amendments to the Stored Communications Act below, a side-by-side comparison of the current law and proposed amendments is included in the Appendix.

Explanation

This amendment would make subsection (a) simpler, more consistent across different types of content data, and easier to apply.

First, it would equalize the protections for *content* information, regardless of whether the content is being used for electronic communications, remote computer processing, or remote storage (under the terminology of the current law).[181] And borrowing a suggestion from Kerr, the amendment would replace the outdated terms "electronic communication service" and "remote computing service" with the broader term "network service provider," greatly reducing the statute's complexity.[182] (In the current Act, content from electronic communication services is governed by subsection (a), while content stored in remote computing services is governed by subsection (b).) As a result, all requests for content information would be consolidated into a single subsection with a single level of protection.

Second, the amendment would require a warrant and probable cause for all disclosures of content information. This uniform demand would replace the current statute's weaker protection for certain types of content (for example, opened e-mail messages and unopened e-mail messages stored for longer than 180 days, which the government may now request using only an administrative subpoena).[183] Traditional Fourth Amendment doctrine, in contrast, protects both unopened and opened letters.[184] Digital content information should be protected at the same level with the same consistency. As noted above, the law's current provisions reflect the communications technologies of the 1980s and have little justification in the Internet age.

Third, revised subsection (a)(2) would close a potentially gaping exemption in the statute: the lack of protection for data stored in remote services that the provider may access for purposes other than storage or remote processing.[185] Removing this exception—currently found in subsection (b)(2)(B)—would ensure the statute's protections extend to data stored in cloud computing services such as Google Docs and Microsoft Office Online and in cloud storage services such as Google Drive, Microsoft OneDrive, and Dropbox. Most or all of these services contain provisions in their terms of ser-

---

181. Remote computer processing is currently housed under 18 U.S.C. § 2703(b) (2013), and treated differently than electronic storage. *Compare id.* § 2703(a) (regulating the disclosure of communications in electronic storage), *with id.* § 2703(b) (regulating the disclosure of communications in a remote computing service).

182. *See* Kerr, *supra* note 137, at 1235.

183. 18 U.S.C. § 2703(a)-(b).

184. *See* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 315 (2015). Fourth Amendment protections transfer from sender to recipient, however, when the letter is delivered. *Id.*

185. *See* 18 U.S.C. § 2703(b)(2)(B) (limiting the section's protections to wire and electronic communications held or maintained "*solely* for the purpose of providing storage or computer processing services to [the] subscriber or customer" (emphasis added)).

vice that grant the service providers some rights to access the contents of the data, often to provide the targeted advertising that funds the services.[186] As a result, the current statute does not necessarily protect content housed in these services, because it protects only communications held "*solely* for the purpose of providing storage or computer processing services to such subscriber or customer."[187]

Finally, the amendment would limit the applicability of the statute to the contents of *nonpublic* communications. The government would therefore retain the ability to request the contents of public communications such as Twitter tweets, publicly accessible Facebook posts, and other content intended for wide distribution. Because these communications are already shared widely, their authors have little expectation of privacy in their contents.[188]

These changes to subsection (a) would broaden the scope of the Stored Communications Act's protection of content information, making it more consistent with the Fourth Amendment's protection of physical documents. The proposal would not unduly hinder government investigations beyond the challenges inherent to traditional investigations. As a result, it would bring the statute into line with the Sixth Circuit's holding in *Warshak*, which determined that the law is unconstitutional as applied to e-mail (and perhaps other forms of electronic communications).[189]

The Revised Statute—18 U.S.C. § 2703(b)

> **(b)~~(c)~~ Records Concerning Network Service. ~~Electronic Communication Service or Remote Computing Service. (1)~~** A governmental entity may require a network service provider ~~provider of electronic communication service or remote computing service~~ to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

186. *See, e.g.*, *Google Terms of Service*, GOOGLE, http://www.google.com/intl/en/policies/terms (last modified Apr. 14, 2014) ("Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.").

187. 18 U.S.C. § 2703(b)(2)(B) (emphasis added). Google's terms of service, for example, require users to provide the company "a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content." *Google Terms of Service*, *supra* note 186.

188. *See* United States v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) ("When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment.").

189. *See supra* text accompanying notes 141-47.

> **(1)**~~**(A)**~~ obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;
>
> **(2)**~~**(B)**~~ obtains a court order for such disclosure under subsection (d) of this section, if the information required by the present request, and by any previous requests made to the same provider during the course of the current investigation, was initially collected by the provider from user activity taking place during a period not exceeding seven cumulative days;
>
> **(3)**~~**(C)**~~ has the consent of the subscriber or customer to such disclosure;
>
> **(4)**~~**(D)**~~ submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or
>
> **(5)**~~**(E)**~~ seeks information under subsection (c) ~~paragraph (2)~~.[190]

Explanation

Revised subsection (b) would incorporate the mosaic theory into the Stored Communications Act to prevent warrantless disclosures of sweeping amounts of metadata. The subsection would require a warrant for all requests to a single provider regarding information collected over a period of at least seven cumulative days. More discrete information requests—that is, requests for information collected over less than seven cumulative days—would remain governed by the current statute's court order and reasonable suspicion requirements. This proposal also would not affect the government's ability to warrantlessly request information made with the consent of the subscriber or customer, concerning telemarketing fraud, or relating to basic subscriber information.

Adopting the mosaic theory in this statutory manner would prevent many of the potential pitfalls that could arise if the Supreme Court were to incorporate the mosaic theory into Fourth Amendment doctrine. And the proposal would address the most important practical questions posed by the mosaic theory's most vocal critic, Kerr[191]:

---

190. The remainder of current subsection (b) would be moved to subsection (c).

191. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 328-43 (2012).

1. What is the "proper reference point for when a mosaic has been created[?]"[192]
2. "[H]ow long must [a surveillance] tool be used before the relevant mosaic is created?"[193]
3. "If the mosaic theory applies to multiple surveillance methods, . . . [should] duration and scale questions . . . be answered in the same way for every method[?]"[194]
4. "[W]hich stages of surveillance [does] the mosaic theory regulate[]: initial data collection, subsequent analysis, or both[?]"[195]
5. Would the mosaic theory apply when multiple agencies request data, either in separate investigations or in joint operations?[196]

By statutorily defining the scope of the mosaic theory's effect on government information requests, this proposal answers these questions. The proposal, particularly subsection (b), is intended to be a prophylactic shield against the privacy danger posed by the government's easy access to individuals' metadata stored with a third party. It does not attempt to perfectly address every possible scenario—an impossible task. Revised subsection (b) would answer Kerr's first three questions somewhat arbitrarily, as follows: First, the proper reference point (under the proposal) for when a mosaic has been created is a defined time period. Second, that period is seven cumulative days. And third, duration and scale questions would be answered identically in every case, regardless of the technological context.

Prophylactic measures and arbitrary thresholds are neither inherently problematic nor without precedent in criminal procedure. For instance, the *Miranda* doctrine prophylactically ensures criminal suspects are aware of their Fifth Amendment right against self-incrimination; *Miranda* warnings are not direct applications of the Fifth Amendment.[197] Similarly, the Supreme Court has held that invocation of the Fifth Amendment right to counsel expires after fourteen days,[198] an entirely arbitrary threshold. The Court did not set this bright-line number to perfectly define the boundaries of the Fifth Amendment right. In-

192. *Id.* at 330.

193. *Id.* at 333.

194. *Id.* at 335.

195. *Id.* at 330.

196. *Id.* at 335-36.

197. *See* New York v. Quarles, 467 U.S. 649, 654 (1984) ("The prophylactic *Miranda* warnings therefore are 'not themselves rights protected by the Constitution but [are] instead measures to insure that the right against compulsory self-incrimination [is] protected.'" (alterations in original) (quoting Michigan v. Tucker, 417 U.S. 433, 444 (1974))). *But see* Dickerson v. United States, 530 U.S. 428, 437-41 (2000) (noting that while the *Miranda* warnings are prophylactic applications of the Fifth Amendment, *Miranda* was nevertheless decided on constitutional grounds).

198. Maryland v. Shatzer, 559 U.S. 98, 110-11, 117 (2010).

stead, the Court's intention was "to avoid the consequence" of "not reach[ing] the correct result most of the time."[199]

Likewise, here, the arbitrary nature of the proposal's seven-day mosaic threshold is a feature, not a bug. A bright-line rule would lend confidence to the government when it requests data, to third parties when they disclose users' information, and to judges when they apply the law. It would also allow individuals to determine whether a data disclosure violated their legal rights. Such a rule, despite its potential to over- and underprotect privacy in some circumstances, is superior to an overly complex scheme that hinders government investigations or to no rule at all, which threatens individuals' privacy.

The proposal also answers Kerr's fourth question: Which stage—collection or analysis—is relevant? To maintain consistency with typical Fourth Amendment searches, the proposal defines the important stage of surveillance as *collection*: service providers' initial collection of information from individuals and the government's later collection of that information from those providers. If the government warrantlessly requests too much information under § 2703(b), that request would be illegal under the revised statute. But in keeping with the sequential nature of Fourth Amendment doctrine,[200] if the government makes multiple requests for information at different times and only the later requests violate the statute, the earlier requests would remain valid. For example, if police request metadata originally collected during a six-day period and later seek additional metadata collected during a separate six-day period, the government could still use the information obtained from the first request. In conjunction with the added suppression remedy, discussed below, this approach would allow other Fourth Amendment doctrines, such as inevitable discovery[201] and fruit of the poisonous tree,[202] to apply as usual.

Finally, this proposal would address Kerr's fifth question: how the mosaic theory would handle multiple requests made by separate officers or agencies conducting either individual investigations or joint operations. It would clarify that requests arising from *separate* investigations would be treated separately, while requests by multiple officers (or agencies) in the *same* investigation would be considered together. While these lines may not always be clear, magistrate judges mulling government requests for court orders and warrants are in a proper position to evaluate those requests on a case-by-case basis, and liti-

---

199. *Id.* at 110 (quoting Coleman v. Thompson, 501 U.S. 722, 737 (1991)) (internal quotation mark omitted).

200. *See* Kerr, *supra* note 191, at 315-20 (describing this approach).

201. *See* Nix v. Williams, 467 U.S. 431, 448 (1984) ("[W]hen . . . the evidence in question would inevitably have been discovered without reference to the police error or misconduct, there is no nexus sufficient to provide a taint and the evidence is admissible.").

202. *See* Wong Sun v. United States, 371 U.S. 471, 484 (1963) ("[E]vidence seized during an unlawful search could not constitute proof against the victim of the search. The exclusionary prohibition extends as well to the indirect as the direct products of such invasions." (citation omitted)).

gants can challenge the validity of magistrates' determinations when appropriate.

Incorporating this mosaic framework into the Stored Communications Act would ensure judicial oversight and guard against government attempts to game the system by making multiple, smaller requests adding up to a larger, mosaic whole.[203] For instance, under this proposal, the government could request information pertaining to a six-day period or to two separate three-day periods (or any other combination of time spans adding up to less than seven days). But the proposal would forbid the government from warrantlessly seeking information collected from Monday through Saturday for an entire month (that is, twenty-four days' worth of information but never in a single seven-day chunk). As a result, this proposal would draw clear boundaries allowing law enforcement officers, judges, and individuals to know whether government requests for information are legitimate or excessive under the statute.

The Revised Statute—18 U.S.C. § 2703(c)

> **(c) Basic Subscriber Information**.—A ~~provider of electronic communication service or remote computing service shall~~ network service provider must disclose to a governmental entity the—
>
> **(1)~~(A)~~** name;
>
> **(2)~~(B)~~** address;
>
> **(3)~~(C)~~ ~~local and long distance telephone connection records, or~~** records of session times and durations of local and long distance telephone calls;
>
> **(4)~~(D)~~** length of service (including start date) and types of service utilized;
>
> **(5)~~(E)~~** telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
>
> **(6)~~(F)~~** means and source of payment for such service (including any credit card or bank account number),

---

203. *See* Matthew Radler, Note, *Privacy Is the Problem:* United States v. Maynard *and a Case for a New Regulatory Model for Police Surveillance*, 80 GEO. WASH. L. REV. 1209, 1236-38 (2012) (recounting a police department's successful effort to avoid an adverse holding based on the mosaic theory by splitting twenty-one days of surveillance into three shorter periods).

> of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under ~~paragraph (1)~~ subsection (b). ~~(3)~~ A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

Explanation

This proposal would move current subsection (b)(2) to subsection (c) to clarify the three-tier relationship of the statute: a warrant requirement for subsection (a), a court order requirement for subsection (b), and a subpoena requirement for subsection (c).

Revised subsection (c) would contain only one substantive change: a limitation on the telephone metadata available to the government using only an administrative subpoena. Specifically, revised subsection (c)(3) would allow the government to request via subpoena only the session times and durations of a subscriber's phone calls, not the telephone numbers of the third parties who received or initiated those calls.[204] As demonstrated in Part II.A, telephone metadata that include numbers dialed can reveal intimate details about an individual's medical history, political activities, religion, and more. This change therefore addresses the mosaic theory as well as Justice Marshall's related concerns in his *Smith v. Maryland* dissent.[205]

Additionally, the word "must" would replace "shall" in the opening paragraph of revised subsection (c), mirroring the restyling of the Federal Rules of Criminal Procedure, Civil Procedure, and Evidence.[206] This change is not intended to be substantive.

2. *A suppression remedy*

The proposed amendment to the Stored Communications Act would also include a new § 2713, titled "Prohibition of use as evidence of disclosed contents and records from network service providers":

> Whenever a network service provider discloses the contents of wire or electronic communication stored in such service, or records concerning such service, no part of the disclosure and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdi-

204. Of course, the government would still be able to request this information consistent with the warrant and court order requirements of revised subsections (a) and (b).

205. 422 U.S. 735, 752 (1979) (Marshall, J., dissenting).

206. *See* FED. R. EVID. 101 advisory committee's note to 2011 amendment (describing the ambiguous nature of the words "shall" and "may").

> vision thereof if the disclosure of that information would be in violation of this chapter.

This language is adapted from 18 U.S.C. § 2515, the suppression remedy for Title III wiretaps.

Adding this suppression remedy to the Stored Communications Act would be good policy, regardless of whether the rest of this proposal is implemented. This change is relatively straightforward and has been endorsed by even critics of the mosaic theory such as Kerr.[207] It makes little sense to treat disclosures that violate the Stored Communications Act differently than typical searches that violate the Fourth Amendment. Adding a suppression remedy would create an additional disincentive against illegitimate government disclosure requests. It would also increase judicial interpretation of the statute because most search and seizure case law stems from defendants' attempts to suppress evidence.[208]

3. *Defining "network service"*

The final change in this proposal is the replacement of the term "remote computing service" with "network service" in 18 U.S.C. § 2711(2):

> the term "network service" ~~"remote computing service"~~ means any ~~the~~ provision to the public of wire or electronic communication, computer storage, or processing services by means of an electronic communications system;

As noted above, removing the distinction between "electronic communication services" and "remote computing services" and combining both terms into a single, unified definition would make the statute simpler. It would also ensure that the Act's protections apply more consistently across different types of online services. This definition for "network service" is similar to the current definition of "remote computing service" but adds "wire or electronic communication" to the list of services included. It also adds "any" before "provision" to clarify that the law's protections should apply broadly. Implementing these changes would ensure that the three tiers of protection described above would govern regardless of the type of network services individuals use. It would strengthen the statutory scheme while allowing for the flexibility to accommodate new types of cloud computing services that have not yet been invented.

---

207. Kerr, *supra* note 137, at 1241-42.

208. *See id.* at 1241 ("[F]ew if any cases exist interpreting the SCA in a routine criminal context . . . . A suppression remedy would guarantee that criminal defendants challenge government and ISP practices under the SCA . . . .").

C. *Alternative Proposals for Amending the Stored Communications Act*

Considering the outdated nature of the Stored Communications Act, it should come as little surprise that this Note is not alone in calling for changes to the statute. While it would be far beyond the scope of this Note to address all such proposals, two in particular stand out. The first is Kerr's set of suggestions in his article *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*.[209] Kerr is one of the most prolific and knowledgeable legal scholars writing about digital privacy issues today—and arguably the mosaic theory's most vocal critic—so his proposal warrants a response. The second is the Email Privacy Act, a bill introduced by Representative Kevin Yoder and cosponsored by a majority of House members.[210] Due to its relative popularity in Congress, this potential legislation presents the likeliest opportunity for amending the law in the short term. Both Kerr's proposal and the Email Privacy Act would move the law in the right direction. Neither, however, provides sufficient protection for citizens' privacy, especially in the area of metadata.

Kerr introduced his suggestions at the end of an article explaining how the Stored Communications Act's individual components work (and, in some cases, interrelate).[211] As a result, his proposals are not focused on advancing any unified goal. Instead, Kerr proposes four discrete amendments to address his various criticisms of the law as written: (1) raising the threshold for government requests for content data, (2) simplifying the statute by combining "remote computing services" and "electronic communication services," (3) repealing 18 U.S.C. § 2701, and (4) modifying the remedies for violations of the statute.[212]

Kerr's first suggestion—raising the threshold for requests for content data—primarily addresses the statute's odd distinction (discussed above) between new, unopened e-mails and e-mails that have been opened or stored for more than 180 days.[213] But instead of advocating for a warrant for all content data, Kerr takes "a cautious middle ground": he suggests requiring a § 2703(d) court order, which demands only a showing of reasonable suspicion (not probable cause).[214] Because this change would eliminate the government's current ability to compel via subpoena the disclosure of the contents of certain online doc-

---

209. *Id.* at 1233-42.

210. H.R. 1852, 113th Cong. (2013); *Cosponsors—H.R. 1852—113th Cong. (2013-2014): Email Privacy Act*, CONGRESS.GOV, https://beta.congress.gov/bill/113th-congress/house-bill/1852/cosponsors (last visited Feb. 23, 2015). A related Senate bill, the Electronic Communications Privacy Act Amendments of 2013, garnered fewer cosponsors and stalled in committee. S. 607, 113th Cong. (2013); *Actions—S. 607—113th Congress (2013-2014): Electronic Communications Privacy Act Amendments of 2013*, CONGRESS.gov, https://beta.congress.gov/bill/113th-congress/senate-bill/607/all-actions (last visited Feb. 23, 2015).

211. *See* Kerr, *supra* note 137, at 1233-42.

212. *Id.* at 1209.

213. *Id.* at 1233-35.

214. *Id.* at 1234-35.

uments, it is clearly a step in the right direction. But it nevertheless fails to provide digital documents the same level of privacy protection paper documents enjoy (and Kerr has subsequently argued for a warrant requirement for content data).[215]

Kerr's second suggestion is to simplify the statute by combining the terms "remote computing service" and "electronic communication service" into a single, broader "network service."[216] As mentioned above, this Note's proposal would adopt this suggestion outright.

Kerr's third suggestion is to repeal 18 U.S.C. § 2701, which provides criminal penalties for accessing documents in an electronic communication service without authorization.[217] This section of the Stored Communications Act, Kerr argues, is almost completely redundant to the Computer Fraud and Abuse Act,[218] and its vague language has confused the courts.[219] Regardless of the merits of this suggestion, it is beyond the scope of this Note, which focuses on the Stored Communications Act's procedural provisions.

Finally, Kerr suggests altering the remedies for violations of the Act. First and foremost, he proposes (as does this Note) incorporating a suppression remedy in criminal cases.[220] Kerr also suggests clarifying under which circumstances civil remedies are available against the government and against service providers.[221] This latter proposal is probably wise—especially in the absence of a suppression remedy—and would be entirely compatible with this Note's proposal.

In contrast to Kerr's proposal, which addresses several largely unrelated problems with the Stored Communications Act, the Email Privacy Act appears to have one main goal: making the statute consistent with *Warshak*'s holding that the Fourth Amendment protects the contents of e-mail communications.[222]

The Email Privacy Act, like both this Note's and Kerr's proposals, would combine the Stored Communications Act's provisions concerning electronic communication services and remote computing services and equalize the protection given to each type of service.[223] In doing so, the Email Privacy Act would remove the current law's distinctions between new, unopened e-mails

---

215. *See* Orin Kerr, *Sixth Circuit Rules that E-mail Protected by the Fourth Amendment Warrant Requirement*, VOLOKH CONSPIRACY (Dec. 14, 2010, 11:30 AM), http://www.volokh.com/2010/12/14/sixth-circuit-rules-that-e-mail-protected-by-the-fourth-amendment-warrant-requirement (judging *Warshak*'s reasoning to be "correct").

216. Kerr, *supra* note 137, at 1235.

217. *Id.* at 1238-41.

218. *See generally* 18 U.S.C. § 1030 (2013).

219. Kerr, *supra* note 137, at 1239-41.

220. *Id.* at 1241.

221. *Id.* at 1241-42.

222. *See generally* H.R. 1852, 113th Cong. (2013).

223. *See id.* § 3. Unlike this Note's and Kerr's proposals, however, the Email Privacy Act does not use a single umbrella term ("network service") to incorporate both types of service into a single definition.

and old or opened e-mails.[224] Going beyond Kerr's recommendation (but matching this Note's), the proposed law would require a warrant for all content disclosures under § 2703(a).[225] And the Email Privacy Act would compel the government to notify users within three days (ten for law enforcement agencies) of obtaining the contents of their communications via a warrant.[226] Despite all of these positive changes, however, the proposed law fails to include a suppression remedy.[227]

Both Kerr's proposed changes and the Email Privacy Act would be positive steps toward bringing digital privacy protections into line with the Fourth Amendment's protections for physical documents. Both would simplify the structure of the law. And both would increase the protection for content disclosures under § 2703(a). But neither goes far enough. Kerr's proposal fails to require a warrant for content disclosures, and the Email Privacy Act fails to include a suppression remedy. Without both a warrant requirement and a suppression remedy, the Stored Communications Act's protections for the *contents* of documents stored in the cloud will lag behind the Fourth Amendment protections for otherwise identical paper documents.

Just as importantly, neither Kerr's proposal nor the Email Privacy Act contains any new protection against government requests for metadata. As the *Maynard* and *Jones* opinions have suggested, and as this Note has shown, extensive metadata records can provide insights into citizens' lives that can be every bit as revealing as the contents of their documents. Proposals to amend the Stored Communications Act without addressing mosaic theory concerns will fail to address one of the greatest—and ever-growing—threats to privacy in the modern era.

CONCLUSION

Technology companies,[228] privacy groups,[229] members of Congress,[230] and even the White House[231] agree: the Stored Communications Act is outdat-

224. *See id.*

225. *Id.*

226. *Id.* This is a significant heightening of the notice requirement. The current law only requires the government to provide users notice when their data is sought through a subpoena or court order, not pursuant to a warrant. 18 U.S.C. § 2703(b) (2013). On the other hand, the Email Privacy Act extends the delayed notice period (when applicable) for law enforcement agencies from 90 days to 180. *Compare* H.R. 1852 § 4, *with* 18 U.S.C. § 2705. Kerr, in contrast, supports reducing the delayed notice period from 90 days to 30. *See* Kerr, *supra* note 137, at 1235.

227. *See generally* H.R. 1852.

228. CARDOZO ET AL., *supra* note 147, at 17-18.

229. *E.g.*, *Don't Let Privacy Law Get Stuck in 1986*, ELECTRONIC FRONTIER FOUND., https://act.eff.org/action/don-t-let-privacy-law-get-stuck-in-1986 (last visited Feb. 23, 2015).

230. *See supra* notes 222-27 and accompanying text.

ed and should be reformed. The Act's protections are based on Reagan-era technologies and do not adequately guard against modern threats to privacy. As a result, many companies now refuse to comply with information requests under the Act and demand warrants before disclosing their customers' data.[232] Indeed, Apple, Facebook, and a number of other major tech companies have gone one step further, announcing that they will inform customers any time the government requests their data unless they receive a judicial gag order.[233] This unstable situation harms consumers, who do not know which competing legal standard companies will follow—the Stored Communications Act or *Warshak*. It also hinders the investigations of law enforcement officers, who may not be able to acquire the information they need for their investigations and who may fear tipping off potential suspects before assembling the evidence needed for a successful prosecution.

Relying on the mosaic theory insights of *Maynard* and the *Jones* concurrences, this Note's proposed amendment to the Stored Communications Act would address the statute's current failings in a measured way. Though the proposal would require the government to obtain a warrant before requesting content information or sweeping amounts of metadata, it would allow law enforcement officers to rely on court orders and subpoenas for more targeted (and less invasive) disclosures. In so doing, it would clarify the government's legal obligations, making the Act easier for the government and magistrate judges to follow and simpler for criminal litigants to understand. Moreover, adding a suppression remedy would allow courts to apply the law to new circumstances, making the statute adaptable to new technologies for years to come.

By statutorily implementing these changes in the manner proposed, the Stored Communications Act would once again protect citizens' online privacy while allowing the government to conduct criminal investigations with clear and reasonable boundaries. And contrary to critics' concerns about the feasibility of implementing the mosaic theory, all of these changes would be compatible with, and would require no fundamental reconfiguration of, existing Fourth Amendment doctrine.

---

231. Press Release, White House, Fact Sheet: Big Data and Privacy Working Group Review (May 1, 2014), http://www.whitehouse.gov/the-press-office/2014/05/01/fact-sheet-big-data-and-privacy-working-group-review.

232. *See supra* text accompanying note 147.

233. Craig Timberg, *Apple, Facebook, Others Defy Authorities, Increasingly Notify Users of Secret Data Demands After Snowden Revelations*, WASH. POST (May 1, 2014), http://wapo.st/1mj01Ni.

APPENDIX
Side-by-Side Comparison of the Current Stored Communications Act and Proposed Amendments

Excerpts from Current Law	*Proposed Amendments*
18 U.S.C. § 2703: Required disclosure of customer communications or records	**18 U.S.C. § 2703: Required disclosure of customer communications or records**
(a) Contents of Wire or Electronic Communications in Electronic Storage.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.	**(a) Contents of Wire or Electronic Communications or Documents Held by Network Service Providers.**—A governmental entity may require the disclosure by a network service provider of— **(1)** the nonpublic contents of a wire or electronic communication; or **(2)** the nonpublic contents of any document held or maintained on that service on behalf of a subscriber of such service, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction.
(b) Contents of Wire or Electronic Communications in a Remote Computing Service.— **(1)** A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this par-	

agraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communica-

tions received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records Concerning Electronic Communication Service or Remote Computing Service.—

(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(b) Records Concerning Network Service.—A governmental entity may require a network service provider to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(1) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(2) obtains a court order for such disclosure under subsection (d) of this section, if the information required by the present request, and by any previous requests made to the same provider during the

	course of the current investigation, was initially collected by the provider from user activity taking place during a period not exceeding seven cumulative days;
(C) has the consent of the subscriber or customer to such disclosure;	**(3)** has the consent of the subscriber or customer to such disclosure;
(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or	**(4)** submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or
(E) seeks information under paragraph (2).	**(5)** seeks information under subsection (c).
(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—	**(c) Basic Subscriber Information**.—A network service provider must disclose to a governmental entity the—
(A) name;	**(1)** name;
(B) address;	**(2)** address;
(C) local and long distance telephone connection records, or records of session times and durations;	**(3)** records of session times and durations of local and long distance telephone calls;
(D) length of service (including start date) and types of service utilized;	**(4)** length of service (including start date) and types of service utilized;
(E) telephone or instrument number or other subscriber	**(5)** telephone or instrument number or other subscriber number or

number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

18 U.S.C. § 2711: Definitions for chapter

As used in this chapter—

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system;

identity, including any temporarily assigned network address; and

(6) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under subsection (b). A governmental entity receiving information under this subsection is not required to provide notice to a subscriber or customer.

18 U.S.C. § 2711: Definitions for chapter

As used in this chapter—

(2) the term "network service" means any provision to the public of wire or electronic communication, computer storage, or processing services by means of an electronic communications system;

18 U.S.C. § 2713: Prohibition of use as evidence of disclosed contents and records from network service providers

Whenever a network service provider discloses the contents of wire or electronic communication stored in such service, or records concerning such service, no part of the disclosure and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.