2015

Corporate Avatars and the Erosion of the Populist Fourth Amendment

Avidan Cover

Corporate Avatars and the Erosion of the Populist Fourth Amendment

*Avidan Y. Cover**

ABSTRACT: Fourth Amendment jurisprudence currently leaves it to technology corporations to challenge court orders, subpoenas, and requests by the government for individual users' information. The third-party doctrine denies people a reasonable expectation of privacy in data they transmit through telecommunications and Internet service providers. Third-party corporations become, by default, the people's corporate avatars. Corporate avatars, however, do a poor job of representing individuals' interests. Moreover, vesting the Fourth Amendment's government oversight functions in corporations fails to cohere with the Bill of Rights' populist history and the Framers' distrust of corporations.

This Article examines how the third-party doctrine proves unsupportable in the big data surveillance era, in which communicating and sharing information through third parties' technology is a necessary condition of existence, and non-content data, such as Internet subscriber information or cell site location information, provides an intimate portrait of a person's activities and beliefs. Recognizing the potential for excessive government surveillance, scholars, courts, and Congress have endorsed corporations as one solution to Executive branch overreach and privacy invasion.

This Article demonstrates through both government and corporate reports that companies have rarely challenged government requests for their users' data. Incentives to cooperate with government surveillance, including highly profitable relationships with government, government regulation of companies, and statutory immunity, make it unlikely that corporations will ever be adequate avatars. This Article further documents how expansive search powers originated in England with the aid of private industry, making corporations dubious guardians of the Fourth Amendment.

* Assistant Professor of Law, Case Western Reserve University School of Law; Director, Institute for Global Security Law and Policy. I am grateful to Jessie Hill, Sharona Hoffman, Lew Katz, Orin Kerr, Raymond Ku, and Cassandra Burke Robertson for their helpful comments. Additional thanks to Andrew Dorchak, Judith Kaul, Lisa Peters, and Hui Wu for their assistance with legal research.

This Article offers three practicable solutions to increase individual agency. First, the third-party doctrine should be limited in order to permit an expectation of privacy in some non-content data. Second, Congress should enact proprietary rights in certain personal data. Finally, technological advances should facilitate individuals' selection of corporations' services and devices that ensure notice of government surveillance and enable direct communication between the people and government over searches and seizures.

I. INTRODUCTION

We live in a surveillance state founded on a partnership between government and the technology industry.[1] Edward Snowden's revelations that law enforcement and intelligence agencies have obtained communications and phone and email records of Internet providers' users cement this reality.[2]

A key feature of the surveillance state is the cooperative relationship between the private sector and the government. The private sector's role is vital to the surveillance both practically and legally. The private sector, of course, provides the infrastructure and tools for the surveillance. It is through the communications on smartphones built by Apple or the videos hosted by YouTube that the government obtains data. Surveillance is further facilitated by arrangements between the government and companies, such as built-in backdoors and informal agreements.

The private sector is also critical to the surveillance state's legality. Under the third-party doctrine, the Fourth Amendment is not implicated when the government acquires information that people provide to corporations, because they voluntarily provide their information to another entity and assume the risk that the entity will disclose the information to the government. Therefore, people do not have a reasonable expectation of privacy in their calling data, or potentially even their emails. As a result, the government does not normally need a warrant to obtain information transmitted electronically.

But the Fourth Amendment is not only a source of protection for individual privacy; it also limits government excess and abuse through challenges by the people. The third-party doctrine removes this vital and populist check on government overreach.

The unsatisfying answer to this constitutional dilemma has been what I describe as the "corporate avatar dynamic." In Internet parlance, avatars refer to characters that represent users in venues as diverse as online games, communities, and discussion groups.[3] But whatever form the avatar takes, the user controls the avatar. In response to critics of surveillance and the third-

1. S*ee* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 6–9 (2008).

2. *See* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3aocoda8-cebf-11e2-8845-d970ccb04497_story.html; Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 AM), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. Just weeks earlier, it was revealed that Verizon acquiesced to government subpoenas of Associated Press reporters' phone data. *See* Charlie Savage & Scott Shane, *Justice Dept. Defends Seizure of Phone Records*, N.Y. TIMES (May 14, 2013), http://www.nytimes.com/2013/05/15/us/politics/attorney-general-defends-seizure-of-journalists-phone-records.html.

3. *See Avatar*, TECHTERMS.COM, http://www.techterms.com/definition/avatar (last visited Mar. 6, 2015).

party doctrine, apologists argue that even if someone does not have a privacy interest in a phone call or Internet data, the third party—Facebook, Sprint, or Twitter—may act as our avatar: The company can assert claims against searches, standing in the shoes of the person.[4] In a similar vein, Congress enacted laws permitting communications providers to challenge directives concerning assistance with government surveillance on their own behalf and on behalf of their subscribers.[5] And courts have upheld the right of third-party service providers to challenge government requests for information on their customers' behalf, with the Supreme Court indicating these challenges fulfill the government-checking purposes of the Fourth Amendment.[6]

Concerned that the forces of government and commerce rule cyberspace, Lawrence Lessig asks: "How do we protect liberty when the architectures of control are managed as much by the government as by the private sector?"[7] Making corporate avatars the primary means of challenging government searches on behalf of people inadequately responds to Lessig's concern.

This Article diagnoses and solves the problem of corporate avatars. Corporations are poor avatars for people. They cannot serve a government-checking function when they have vested interests in cooperating with the government. Moreover, maintaining the Fourth Amendment's government-checking function in corporate avatars runs counter to the Framers' distrust of powerful corporations.

This Article proceeds in five parts. Part II provides a brief overview of the third-party doctrine and its application to big data. Part III describes the corporate avatar dynamic. Part IV addresses corporate avatars' limitations and shows few instances of corporate challenges to government requests for user data. Part V shows how technology corporations are not likely to challenge government surveillance requests, and even less likely to make effective arguments asserting their individual customers' rights, because of their government connections, the legal constraints on transparency and disclosure, and their immunity for complying with the government. Part V also explains how the objectives of a populist Fourth Amendment are undermined by the substitution of corporations for the people. Part VI recommends notice to the user as the primary mechanism for returning to a populist Fourth Amendment that properly limits government overreach. The theoretical underpinnings for a notice regime require reconceiving people's relationship to data as a proprietary one and limiting the third-party doctrine. The Article concludes by proposing a "machine-to-machine mechanism" by which peoples' privacy and notice preferences are communicated to both the

4. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 598–600 (2009).

5. *See* FISA Amendments Act of 2008, 50 U.S.C. § 1881a(h)(4), (6) (2012).

6. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1154–55 (2013).

7. LAWRENCE LESSIG, CODE: VERSION 2.0, at xv (2006).

tech companies and the government, thereby encouraging corporate enforcement of privacy and deterring government overreach.

II. THE THIRD-PARTY DOCTRINE AND BIG DATA

The third-party doctrine comes from conceiving absolute secrecy to be the bedrock of privacy under the Fourth Amendment. That narrow view of privacy, however, is increasingly untenable in an era in which virtually all personal information is disclosed to third parties. The doctrine is also predicated on the conceit that individuals voluntarily share their information with third parties—even though disclosing personal information is a necessary part of today's society. Consequently, individuals' shared data do not receive Fourth Amendment protection against government surveillance.

A. ORIGINS OF THE THIRD-PARTY DOCTRINE

For our purposes, the critical, early third-party doctrine cases are *United States v. Miller*[8] and *Smith v. Maryland*.[9] These cases build on earlier case law, which held that words spoken to an informant receive no Fourth Amendment protection.[10]

In *Miller*, the Supreme Court upheld a whiskey distiller's conviction for unpaid taxes based, in part, on subpoenaed bank records, which were obtained without a court order or notice to the distiller.[11] The Court held that Miller had no Fourth Amendment interest in his bank records.[12] He did not have a legitimate expectation of privacy in the records because they were "not confidential communications but negotiable instruments to be used in commercial transactions."[13] Moreover, the majority reasoned, Miller "voluntarily conveyed [the information] to the banks and exposed [it] to their employees in the ordinary course of business."[14] The Court explained that Miller had assumed the risk that the bank would give his account records to

8. United States v. Miller, 425 U.S. 435 (1976).

9. Smith v. Maryland, 442 U.S. 735 (1979).

10. *See* United States v. White, 401 U.S. 745, 750–51 (1971); Hoffa v. United States, 385 U.S. 293, 300–03 (1966); Lewis v. United States, 385 U.S. 206 (1966). Eleven states have not embraced the third-party doctrine. State courts often interpret their state constitutions to afford privacy to information transmitted to third parties. *See* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 395–99 & nn.118–28 (2006) (cataloguing states and their case law rejecting federal third-party doctrine); *see also, e.g.*, State v. McAllister, 875 A.2d 866, 873 (N.J. 2005) (holding that the New Jersey state constitution affords privacy expectations in bank records); State v. Hunt, 450 A.2d 952, 956–57 (N.J. 1982) (holding that telephone number records are entitled to the state constitution's privacy protections). Henderson identifies another ten states, which he believes might reject the third-party doctrine. *See* Henderson, *supra*, at 400–05 & nn.129–38.

11. *Miller*, 425 U.S. at 437–39.

12. *Id.* at 440.

13. *Id.* at 442.

14. *Id.*

the government when he deposited money there.[15] Moreover, the Court held, Miller did not need to receive notice of the subpoenas.[16]

In *Smith*, the Court upheld a robbery conviction that was based on a pen register of phone numbers the defendant had dialed.[17] The police did not obtain a warrant or court order but simply asked the phone company to install the pen register.[18] The Court held that this was not a search under the Fourth Amendment, and therefore, did not require a warrant.[19]

The Court distinguished *Katz v. United States*, in which it held that it was a search when the government attached a listening device to a phone booth to monitor people's conversations.[20] Unlike the instrument in *Katz*, "pen registers do not acquire the contents of communications."[21] The Court expressed "doubt that people in general entertain any actual expectation of privacy in the numbers they dial."[22] The Court observed that people must know they are providing the numbers to the phone company and that the phone company records these numbers.[23]

But even if the person had held a subjective expectation of privacy in the phone numbers he dialed, the third-party doctrine meant that society did not recognize this expectation as reasonable. Citing the informant cases and *Miller*, the Court explained that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[24] By using the phone, a person "assume[s] the risk that the company would reveal to police the numbers he dialed."[25] Holding that the defendant could not have harbored a legitimate expectation of privacy in the numbers he dialed, the Court held the installation and use of the pen register was not a search and did not require a warrant.[26] *Miller* and *Smith* are powerful precedents and have diminished individual privacy in the big data era.

B. BIG DATA

"Big data" describes both the massive quantity of information about people's communications and behavior, and the range of analysis that can be

15. *Id.* at 443.

16. *Id.* at 443 & n.5.

17. Smith v. Maryland, 442 U.S. 735, 737, 745–46 (1979). A pen register records the phone numbers dialed but does not capture the content of communications. *See id.* at 736 n.1.

18. *Id.* at 737.

19. *Id.* at 745–46.

20. *Id.* at 739–40 (citing Katz v. United States, 389 U.S. 347, 353 (1967)).

21. *Id.* at 741 (emphasis omitted).

22. *Id.* at 742.

23. *Id.* at 742–43. The Court acknowledged "subjective expectations cannot be scientifically gauged," but was incredulous that phone users could believe the number they dial would be secret. *Id.* at 743.

24. *Id.* at 743–44.

25. *Id.* at 744.

26. *Id.* at 745–46.

applied to the information, from which conclusions are drawn.[27] The big data era has come about through "digitization," which entails "making analog information readable by computers, which also makes it easier and cheaper to store and process."[28] Big data's vast array of communications includes "large, diverse, complex, longitudinal, and/or distributed data sets generated from instruments, sensors, Internet transactions, email, video, click streams, and/or all other digital sources available today and in the future."[29] Big data is also historical and essentially permanent.[30]

Digital data double almost every three years.[31] The quantity of data today amounts to each person on the globe having 320 times the information thought to have been held in the great Library of Alexandria.[32] The size of the data sets permits the signature definitional aspect of big data—inferences and predictions about individuals' behavior, be it shopping, voting, or breaking the law.[33]

Technology companies' primary product is their users' personal information.[34] Big data permits personalizing information and services.[35] But individualized products and advertising require the person to share personal

27. *See* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., EXEC. OFFICE OF THE PRESIDENT, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE, at ix (2014), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

28. VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 15 (2013).

29. NAT'L SCI. FOUND. & NAT'L INSTS. OF HEALTH, CORE TECHNIQUES AND TECHNOLOGIES FOR ADVANCING BIG DATA SCIENCE & ENGINEERING (BIG DATA) 5 (2012), *available at* http://www.nsf.gov/pubs/2012/nsf12499/nsf12499.pdf.

30. *See* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 27, at 40 ("[D]ata, once created, are permanent. . . . [T]heir continued *existence* is best considered conservatively as unalterable fact."); ERIC SCHMIDT & JARED COHEN, THE NEW DIGITAL AGE: RESHAPING THE FUTURE OF PEOPLE, NATIONS AND BUSINESS 55 (2013) ("Near-permanent data storage will have a big impact on how citizens operate in virtual space. There will be a record of all activity and associations online, and everything added to the Internet will become part of a repository of permanent information.").

31. MAYER-SCHÖNBERGER & CUKIER, *supra* note 28, at 9.

32. *Id.*

33. *See id.* at 12 ("[I]t's about applying math to huge quantities of data in order to infer probabilities . . . ."); *id.* at 55 ("Predictions based on correlations lie at the heart of big data."); PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 27, at 2.

34. *See* ELI PARISER, THE FILTER BUBBLE: WHAT THE INTERNET IS HIDING FROM YOU 6 (2011) ("You're getting a free service, and the cost is information about you. And Google and Facebook translate that pretty directly into money." (quoting Chris Palmer of the Electronic Frontier Foundation) (internal quotation marks omitted)).

35. SCHMIDT & COHEN, *supra* note 30, at 23 (describing personalization as the "key advance ahead"); SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING (AND WHY WE SHOULD WORRY) 183–84 (2011). *See generally* PARISER, *supra* note 34.

information, and lots of it.[36] There is, as Yahoo! CEO Marissa Mayer and Supreme Court Justice Samuel Alito have separately observed, a trade-off.[37]

We certainly benefit from big data. Amazon recognizes profiles of users when they log on and recommends books based on their shopping history. When those users turn to the *Washington Post*, ads for products that they browsed on another site show up next to news articles.[38] Google searches for the flu provide health authorities' real-time information about an epidemic outbreak.[39]

But big data has its drawbacks. Target stores can determine through data analytics that a customer's shopping selections indicate she is pregnant—a conclusion the store can reach even before anyone else knows.[40] Searches and shopping patterns might affect consumers' mortgage rates and price quotes.[41] And the third-party doctrine allows the government to access these data—both the raw information and analyses of users' data. The Supreme Court has recently expressed concerns that government access to big data may violate the Fourth Amendment.[42]

In *United States v. Jones*, the Court struck down the warrantless use of a global positioning satellite ("GPS") device to track a criminal suspect's car.[43] Though ultimately decided on trespass grounds, the long-term GPS surveillance raised questions for a majority of the Justices about what

36. *See* PARISER, *supra* note 34, at 16 ("Personalization is based on a bargain. In exchange for the service of filtering, you hand large companies an enormous amount of data about your daily life—much of which you might not trust friends with.").

37. VAIDHYANATHAN, *supra* note 35, at 87 ("In all cases it's a trade-off, right, where you will give up some of your privacy in order to gain some functionality, and so we really need to make those trade-offs really clear to people, what information are we using and what's the benefit to them, and then ultimately leave it to user choice." (quoting former Google vice-president Marissa Mayer) (internal quotation marks omitted)); *see also* United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring) ("New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile.").

38. *See* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 27, at 11–13 (listing examples of current and future applications of big data).

39. JARON LANIER, WHO OWNS THE FUTURE? 110 (2013) (describing the analysis of Google word searches to determine flu virus hotspots in real time); MAYER-SCHÖNBERGER & CUKIER, *supra* note 28, at 1–2 (describing the same, specifically for the H1N1 virus).

40. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

41. NAT'L CONSUMER LAW CTR., BIG DATA: A BIG DISAPPOINTMENT FOR SCORING CONSUMER CREDIT RISK 27–28 (2014), *available at* http://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf.

42. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2492–95 (2014) (holding unconstitutional the warrantless search of a cell phone incident to an arrest due, in part, to the cell phone's vast storage capacity, its historical record of data, the variety of data it may hold, and its widespread usage); City of Ontario, Cal. v. Quon, 560 U.S. 746, 760 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy.").

43. United States v. Jones, 132 S. Ct. 945, 948–49 (2012).

surveillance the Fourth Amendment countenances.[44] Justice Sonia Sotomayor questioned the continuing validity of the third-party doctrine in light of big data.[45] She expressed "doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year."[46] Until the doctrine's demise, however, law enforcement and intelligence agencies can access the personal information in big data, often without a warrant and its attendant protections of the probable cause standard and independent judicial review, upsetting the Fourth Amendment's purposes of democratic accountability and limited powers of government.[47]

C. THE THIRD-PARTY DOCTRINE IN THE BIG DATA ERA

The Internet has not changed the third-party doctrine and its assumption of the risk rationale.[48] As one lower court phrased it, "voluntary disclosure" is "built directly into the architecture of the Internet," leading to a loss of users' Fourth Amendment protection.[49] The following Subparts discuss how courts apply the doctrine to various data.

1. Internet Subscriber Information

Federal courts generally agree that people have no expectation of privacy in the subscriber information they submit to an Internet service provider

44. *Id.* at 964 (Alito, J., concurring) ("[L]onger term GPS monitoring in investigations of most offenses impinges on expectations of privacy."); *see id.* at 955 (Sotomayor, J., concurring) (quoting Justice Alito's concurrence).

45. *Id.* at 957 ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." (citing Smith v. Maryland, 442 U.S. 735, 742 (1979); United States v. Miller, 425 U.S. 435, 443 (1976))).

46. *Id.*; *see also id.* at 956 ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

47. *See id.* at 956 (noting "the Fourth Amendment's goal to curb arbitrary exercises of police power to and prevent a too permeating police surveillance" (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)) (internal quotation marks omitted)).

48. *See, e.g.*, United States v. Graham, 846 F. Supp. 2d 384, 399 (D. Md. 2012) (noting that "courts have extended the third-party doctrine to . . . inter alia, credit card statements, electric utility records, motel registration records, and employment records" (citing United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008))).

49. *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 133 (E.D. Va. 2011).

("ISP").[50] Courts often analogize names, email addresses, and websites visited to phone numbers obtained via a pen register.[51]

In *United States v. Forrester*, for example, the United States Court of Appeals for the Ninth Circuit found that computer surveillance was "constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*."[52] Analogizing to *Smith*, the court determined that "e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by [ISPs] for the specific purpose of directing the routing of information."[53] Moreover, the court reasoned, users voluntarily turn over the data to servers.[54]

2. Cell Site Location Information

The majority of federal courts have held that the third-party doctrine applies to cell site location information ("CSLI").[55] The United States Court of Appeals for the Fifth Circuit, for example, determined that CSLI fell within the third-party doctrine because "[t]he cell service provider collects and stores historical cell site data for its own business purposes."[56] It does not obtain the information at the government's behest.[57]

50. *See* United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (collecting cases); *see also* United States v. Christie, 624 F.3d 558, 573–74 (3d Cir. 2010); Rehberg v. Paulk, 611 F.3d 828, 843 (11th Cir. 2010); United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010); Guest v. Leis, 255 F.3d 325, 335–36 (6th Cir. 2001). State courts that do not endorse the third-party doctrine, however, have held that people have a reasonable expectation of privacy in the Internet subscriber information they convey to third-party providers. *See, e.g.*, State v. Reid, 945 A.2d 26, 28 (N.J. 2008).

51. United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007).

52. *Id.* at 510.

53. *Id.*

54. *Id.*

55. *See, e.g.*, United States v. Graham, 846 F. Supp. 2d 384, 400 (D. Md. 2012) (collecting cases); United States v. Benford, No. 2:09-CR-86, 2010 WL 1266507, at *3 (N.D. Ind. Mar. 26, 2010); United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008). Some of these same courts have, however, acknowledged that the use of cell tower triangulation to determine the precise location of people in private locations could implicate the Fourth Amendment. *See, e.g.*, *Suarez-Blanca*, 2008 WL 4200156, at *11. The Supreme Court's finding in *Riley v. California*, that CSLI implicates privacy concerns, is already affecting some lower courts' analyses. Riley v. California, 134 S. Ct. 2473, 2490, 2492 (2014). *Compare* Tracey v. State, 152 So. 3d 504, 524–26 (Fla. 2014) (relying, in part, on *Riley* in holding that the use of CSLI to track individuals constitutes a search under the Fourth Amendment), *with* United States v. Guerrero, 768 F.3d 351, 359 (5th Cir. 2014) (holding that CSLI does not implicate the Fourth Amendment and that "*Riley* does not unequivocally overrule" the Fifth Circuit's CSLI precedent in *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013)), *and* United States v. Martinez, No. 13CR3560-WQH, 2014 WL 5480686, at *4 (S.D. Cal. Oct. 28, 2014) (rejecting the application of *Riley* to CSLI).

56. *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 611.

57. *Id.* at 612.

The Fifth Circuit found that, because users know that the information is provided based on the company's disclosure policies, they provided their CSLI information voluntarily.[58] The court contended that users could have chosen a cell phone provider that does not retain CSLI, or chosen not to make the call.[59]

Some federal courts, however, do not apply the third-party doctrine to CSLI. When the government applied for a court order under the Stored Communications Act ("SCA"),[60] which would have required a cellular phone provider to disclose a customer's CSLI, the United States Court of Appeals for the Third Circuit distinguished the cell phone customer's relationship to the cellular phone company from the relationships in *Smith* and *Miller*.[61] In contrast to the Fifth Circuit, the court determined that the customer had not voluntarily shared his CSLI because customers do not know their CSLI is collected and stored.[62]

Perhaps more important to the Third Circuit, cell phone carriers can locate phones within 50 meters of a call.[63] One district court similarly held that the third-party doctrine should not apply to *cumulative* CLSI because it constituted surveillance of "movements over a considerable time period."[64] This level of detail would, according to Judge Nicholas Garaufis, "implicate sufficiently serious protected privacy concerns" similar to those involved with the content of email communications.[65]

Courts that resist applying the third-party doctrine to CSLI tend to focus on the nature of the privacy intrusion presented by prolonged and pervasive surveillance conducted through acquisition of CSLI, rather than parsing the voluntariness of the disclosure.[66] As Judge Garaufis explained, "there are

58. *Id.* at 613; *see also Guerrero*, 768 F.3d at 358–59 (relying on *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 612–13, 615).

59. *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 613.

60. Stored Communications Act § 201, 18 U.S.C. § 2703(d) (2012).

61. *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317–18 (3d Cir. 2010); *see also* United States v. Davis, 754 F.3d 1205, 1216–17 (11th Cir. 2014), *vacated*, 573 F. App'x 925 (11th Cir. 2014).

62. *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 317–18.

63. *Id.* at 318.

64. *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011). In this case, the cell-phone-located records covered "at least 113 days." *Id.* at 114, 118, 127.

65. *Id.* at 126.

66. *See id.* at 117–19, 126 (citing United States v. Maynard, 615 F.3d 544, 555–68 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012)); *In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 844 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013); *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 585–89, 592–94 (E.D.N.Y. 2010), *rev'd*, No. 10-MC-0550 (E.D.N.Y. Nov. 29, 2010).

circumstances in which the legal interest being protected from government intrusion trumps any actual belief that it will remain private."[67]

3. Email Contents

Unlike Internet subscriber information, courts are more inclined to hold that Internet users have a reasonable expectation of privacy in their emails.

In *United States v. Warshak*, the United States Court of Appeals for the Sixth Circuit held that an Internet user has "a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through a commercial ISP."[68] Therefore, the court held, "[t]he government may not compel" access to the email "without first obtaining a warrant."[69] As a result, the court held that the portions of the SCA that permitted the warrantless collection of email were unconstitutional.[70]

In its analysis, the Sixth Circuit first found that Warshak had an actual expectation of privacy in the contents of his email because they contained his "entire business and personal life."[71] The court contrasted the "confidential communications" in Warshak's emails with the "simple business records" in *Miller*.[72] The court also stressed that the bank was the intended recipient of the records while the ISP was an "intermediary."[73]

The court then considered whether the expectation of privacy in email communications is a reasonable one. Noting the "prominent role that email has assumed in modern communication," the court observed that email "provides an account of its owner's life."[74] As a result, access to a person's email gives the government "the ability to peer deeply into his activities."[75] Thus, the court held, the Fourth Amendment was implicated, rendering the SCA's lack of a warrant requirement for collecting email unconstitutional.[76]

67. *In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d at 124.

68. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (quoting Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007)) (internal quotation marks omitted).

69. *Id.*

70. *Id.*; *see also* 18 U.S.C. § 2703(a)–(f) (2012). The ISP provided the government with over 27,000 emails. *Warshak*, 631 F.3d at 283. Warshak received notice of the ex parte order and subpoena more than a year later. *See id.*

71. *Id.* at 284 (quoting Brief of Appellants Steven Warshak, Harriet Warshak, and TCI Media, Inc. at 40, *Warshak*, 631 F.3d 266 (No. 08-3997), 2009 WL 1581797) (internal quotation marks omitted).

72. *Id.* at 288 (internal quotations omitted) (citing United States v. Miller, 425 U.S. 435, 442 (1976)).

73. *Id.*

74. *Id.* at 284.

75. *Id.*

76. *Id.* at 288.

4. Telephony Metadata

Applicability of the third-party doctrine explains lower courts' differing judgments on the constitutionality of the government's bulk telephony metadata collection under the Foreign Intelligence Surveillance Act ("FISA"). Section 215 of the USA PATRIOT Act amended FISA to authorize the government to seek orders "requiring the production of any tangible things" in connection with foreign intelligence surveillance and investigations.[77] The law also removed restrictions on the types of businesses that could be served and the requirement that the surveillance target be a foreign power or its agent.[78]

Pursuant to section 215, the government has asserted its authority since May 2006 to obtain classified ex parte orders from the Foreign Intelligence Surveillance Court ("FISC") directing telecommunications service providers to provide the National Security Agency ("NSA") with the telephony metadata of *all* calls dialed within the United States.[79] "Telephony metadata" includes all calls' "originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc., trunk identifier, telephone calling card numbers, and time and duration of call."[80] It "does not include the substantive content of any communication . . . or the name, address, or financial information of a subscriber."[81]

The majority of courts have found that the telephony metadata program does not implicate Fourth Amendment privacy. Relying on *Smith*, they have

77. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. §§ 1861–1862 (2012)).

78. *See* 50 U.S.C. § 1861(b)(2)(A)(iii); *see also infra* text accompanying note 131.

79. *See In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc., No. BR-13-80, slip op. at 2 (FISA Ct. Apr. 25, 2013); *see also* Siobhan Gorman et al., *U.S. Collects Vast Data Trove: NSA Monitoring Includes Three Major Phone Companies, as Well as Online Activity*, WALL ST. J. (June 7, 2013, 9:25 AM), http://www.wsj.com/news/articles/SB10001424127887324299104578529112289298922 (stating that AT&T and Sprint have been receiving similar FISA orders for seven years); Lara Jakes, *FISA Court Approves Continued U.S. Phone Surveillance*, HUFFINGTON POST (Sept. 18, 2013, 5:12 AM), http://www.huffingtonpost.com/2013/07/19/fisa-court-approves-surveillance_n_3625610.html (reporting on the renewal of Verizon's FISA order).

80. *In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc.*, No. BR-13-80, slip op. at 2 (internal parentheses omitted).

81. *Id.* Comprehensive descriptions of the metadata collection program may be found in THE PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD 79–129 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf; *see also* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 21–36 (2014), *available at* http://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program-2.pdf.

held that the metadata are "voluntarily" conveyed to the third-party telecommunications provider.[82] Some of the courts noted that "what metadata is has not changed," and that the increased volume of collected metadata has no constitutional significance.[83]

However, Judge Richard Leon distinguished the NSA bulk telephony metadata program from the pen register in *Smith*.[84] Judge Leon noted four significant differences between *Smith* and the NSA program. First, unlike the 13-day operation of the pen register in *Smith*, the metadata program captured data over the course of more than five years.[85] Second, unlike the relationship between the police and the third party in *Smith*, the phone company and the government functioned as "a joint intelligence-gathering operation."[86] Third, the bulk telephony metadata program's technological capabilities far exceed the pen register, rendering *Smith* largely irrelevant as a precedent.[87] Finally, Judge Leon found that the increase in phone ownership and usage enables the government to obtain more data and details about peoples' lives, leading to a greater expectation of privacy that society should consider reasonable.[88] But Judge Leon's opinion is the outlier.

The continuing acceptance of the third-party doctrine raises questions about whether the government-limiting objectives of the Fourth Amendment can be realized in the big data era. Because an individual doesn't have a reasonable expectation of privacy in information conveyed through the third party, she has no Fourth Amendment right to assert. In addition, the individual is rarely provided notice of the request for information or the fact that it is shared with the government. Thus, it is usually left to the tech corporation to resist government requests for users' data.

82. *See* Smith v. Obama, 24 F. Supp. 3d 1005, 1007 (D. Idaho 2014); Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 751–52 (S.D.N.Y. 2013); United States v. Moalin, No. 10cr4246-JM, 2013 WL 6079518, at *6 (S.D. Cal. Nov. 18, 2013); *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things, No. BR 14-01, slip op. at 11–12 (FISA Ct. Mar. 20, 2014); *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 13-158, slip op. at 4–6 (FISA Ct. Oct. 11, 2013); *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573, at *2–3 (FISA Ct. Aug. 29, 2013).

83. *Am. Civil Liberties Union*, 959 F. Supp. 2d at 752 (quoting Klayman v. Obama, 957 F. Supp. 2d 1, 35 (D.D.C. 2013)) (internal quotation marks omitted); *In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things*, No. BR 14-01, slip op. at 19–20; *In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Redacted]*, No. BR 13-109, 2013 WL 5741573, at *3.

84. *Klayman*, 957 F. Supp. 2d at 32–37.

85. *Id.* at 32.

86. *Id.* at 33.

87. *Id.*

88. *Id.* at 33–36.

III. THE CORPORATE AVATAR DYNAMIC

This Part describes the corporate avatar dynamic. Defenders of the third-party doctrine argue that even if an individual cannot challenge certain electronic surveillance, the electronic communications providers may assert the individual's privacy rights and keep the government in check. Thus, the corporation—the third party—becomes the individual's avatar.

A. THE INEVITABLE CONSEQUENCE OF THE THIRD-PARTY DOCTRINE

Orin Kerr argues that third parties that hold customer information can help limit the threat to civil liberties posed by the third-party doctrine by asserting their own rights and that of their customers.[89] When the customer's privacy interests and the business's financial interests align, the third-party business has a clear incentive to challenge government requests for customer information.[90] Thus, Kerr concludes, even without Fourth Amendment protection due to the third-party doctrine, the possibility that third-party businesses will fight the requests may deter government overreach.[91]

To be sure, there are cases in which third parties challenge subpoenas seeking their customers' business records. In addition, tech companies have challenged a small number of government requests for user data in the criminal and national security context.[92] Although these instances of corporate resistance appear more anomalous than the norm, tech companies

89. Kerr does not argue that service providers should be the primary means by which government searches are challenged. Rather, he contends that such challenges are one of several ways in which the third-party doctrine may be limited. *See* Kerr, *supra* note 4, at 595–600. Kerr identifies other alternative privacy protections for records shared with third parties, including statutes and common law privileges, such as attorney-client privilege. *Id.* at 596–98. I question the efficacy of these protections, however, because of the statutes' inadequate notice to individuals and incentives for service provider cooperation with the government, and the limited instances in which common law privileges may apply. Jon Michaels has also proposed that, in the intelligence context, corporations should be legally compelled to play a gatekeeping function, requiring the Executive branch to comply with all legal requirements, such as warrants or subpoenas, before providing information. *See* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 950–52 (2008). Michaels, however, claims that his proposal does not address information falling under the third-party doctrine. *See id.* at 952 n.222. But his insertion of the private sector into a government-checking role raises the same concerns as the corporate avatar dynamic. *See infra* Part V.

90. Kerr, *supra* note 4, at 598. In addition to financial incentives that may prompt Internet companies to seek the protection of user privacy, some see a "libertarian streak" in Internet companies that predisposes them to resist data requests on their users' behalf. *See* Claire Cain Miller, *Secret Court Ruling Put Tech Companies in Data Bind*, N.Y. TIMES (June 13, 2013), http://www.nytimes.com/2013/06/14/technology/secret-court-ruling-put-tech-companies-in-data-bind.html.

91. Kerr, *supra* note 4, at 600. Kerr does not argue companies will always fight government requests for information. But he maintains that the frequent alignment of customers' privacy interests and businesses' financial interests will be "a substantial deterrence" of government excess. *See id.*

92. *See infra* Part IV.A.

have increased their opposition to government requests for user data since the Snowden leaks.[93] But the companies' own interests—not the customer's rights—motivate this opposition. That distinction may mean arguments come less frequently, and take on a different form and scope.[94] In addition, the cases demonstrate diverse corporate responses to government requests for user data—from cooperation to negotiation to litigation.[95]

B. JUDICIAL DISCUSSION OF THE CORPORATE AVATAR DYNAMIC

Courts also have embraced the corporate avatar dynamic. At first glance, this may be seen as buttressing individual rights, because it guards against government overreaching made possible by the third-party doctrine. But courts readily identify the providers' capacity, and their failure, to challenge searches as evidence that the search is legitimate. This ignores the many factors that explain why commercial providers rarely oppose government searches. Thus, judicial acceptance of the corporate avatar dynamic is a pyrrhic victory at best for individual rights.

In *In re Directives [Redacted] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, the Foreign Intelligence Surveillance Court of Review ("FISCR") held that an amendment to FISA granted service providers a cause of action to include claims for their customers' Fourth Amendment violations.[96] The service provider, now identified as Yahoo!,[97] had refused to comply with a directive requiring it to assist in warrantless surveillance of its customers.[98]

The court held that Yahoo! met the constitutional requirements of standing because it would sustain an injury by having "to facilitate the government's surveillances of its customers . . . caused by the government through the directives," which could be redressed by the court.[99] The court found that Congress's explicit provision of a right to challenge the legal directive overcame the prudential limitation on standing for asserting the rights of third parties.[100] Accordingly, Yahoo! could bring a "Fourth

93. *See infra* Parts IV.A, V.B.

94. *See infra* Part IV.C.

95. *See infra* Part IV.

96. *In re* Directives [Redacted] Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1009 (FISA Ct. Rev. 2008); *see also* Protect America Act of 2007, Pub. L. No. 110-55, § 2, 121 Stat. 552, 554, *repealed by* FISA Amendments Act of 2008, Pub. L. No. 110-261, § 403(a)(1)(A), 122 Stat. 2436, 2473 (2008) (codified as amended at 50 U.S.C. § 1881a(a), (c)(2) (2012)) (providing that a service provider that receives a directive "may challenge the legality of that directive").

97. Miller, *supra* note 90.

98. *In re Directives [Redacted] Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d at 1007–08.

99. *Id.* at 1008.

100. *Id.* at 1008–09.

Amendment claim on behalf of its customers."[101] The court ultimately ruled, however, that the warrantless surveillance did not violate the Fourth Amendment.[102]

In *Clapper v. Amnesty International USA*, the Supreme Court invoked the corporate avatar dynamic as a partial basis to deny standing to individual plaintiffs who sought to challenge government surveillance under section 702 of FISA.[103] The plaintiff reporters, lawyers, and human rights advocates claimed section 702 violated their Fourth Amendment rights because it authorized surveillance without a showing of probable cause that the target was a foreign power or agent of a foreign power, and did not require the government to identify the nature and location of the surveillance.[104] The Court ruled that the plaintiffs lacked standing because their claims were speculative and any harm they sustained by trying to avoid being overheard was of their own making.[105]

Responding to contentions that its holding would "insulate the government's surveillance activities from meaningful judicial review," the Court contended meaningful review was still possible.[106] An electronic communications service provider directed by the government to help with surveillance could still challenge the directive's legality in court.[107]

Clapper thus illustrates the Supreme Court's approval of the corporate avatar dynamic: the positioning of the tech company in place of the individual to initiate judicial review and act as a check on government. During oral argument, however, Justice Ruth Bader Ginsburg voiced skepticism that an electronic communications provider would challenge surveillance requests.[108] Her skepticism was not unwarranted. At the time, *Directives* was the only

101. *Id.* at 1009.

102. *Id.* at 1012, 1016.

103. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1154–55 (2013). Section 702 of FISA authorizes "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information," based on "a determination by the Attorney General and the Director of National Intelligence" that without the order "intelligence important to the national security of the United States" will otherwise "be lost." *See* FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2438 (codified as amended at 50 U.S.C. § 1881a(a), (c)(2) (2012)).

104. *Clapper*, 133 S. Ct. at 1145–46.

105. *Id.* at 1146–53.

106. *Id.* at 1154 (citation omitted) (internal quotation marks omitted).

107. *Id.* at 1155 (citing *In re Directives [Redacted] Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d at 1006–16); *id.* at 1154 (citing 50 U.S.C. § 1881a(h)(4), (6)). The Court rejected the plaintiffs' lack of judicial review as a basis for their standing argument on other grounds, including that challenges to surveillance might be raised in court if the government introduces information gleaned from the surveillance. *Id.* at 1154; *see also* United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *1, *27 (D. Or. June 24, 2014) (quoting the government's Supplemental FISA Notification) (holding section 702 to be "reasonable under the Fourth Amendment").

108. Oral Argument at 4–6, *Clapper*, 133 S. Ct. 1138 (No. 11-1025), 2012 WL 5305254, at *4–6.

instance in which a provider had opposed a FISA surveillance directive.[109] And, as Justice Ginsburg noted, that challenge was unsuccessful.[110]

More recently, a court invoked the corporate avatar dynamic as a sword, rather than as a shield. Addressing the legality of the government's bulk phone metadata collection program, Judge Claire Eagan held that the Fourth Amendment did not cover the production of telephony metadata under FISA section 215, a matter she considered resolved by *Smith*.[111]

Though the individual telephone user did not have a legitimate expectation of privacy because she communicated the information to a third party, Judge Eagan invoked the service provider's statutorily provided right to challenge the government request to support the program's constitutionality.[112] Judge Eagan observed that no providers that received an order to produce the metadata challenged the program's legality, thus supporting its legitimacy.[113]

The simultaneous recognition of a corporation's right to challenge requests for information on its customers' behalf and inference that failing to exercise that challenge reflects the requests' legality demonstrate the dangers

109. Letter from the Honorable Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to Senator Patrick J. Leahy, Chairman, U.S. Senate Comm. on the Judiciary 7–8 (July 29, 2013) [hereinafter Letter from Judge Walton], *available at* http://www.uscourts.gov/uscourts/courts/fisc/honorable-patrick-leahy.pdf. As early as January 2009, however, it appears that Sprint raised questions about a FISA order, leading to an amended order regarding its legal conclusions. *See* Charlie Savage, *Phone Company Pushed Back Against N.S.A.'s Data Collection, Court Papers Show*, N.Y. TIMES (May 14, 2014), http://www.nytimes.com/2014/05/15/us/politics/phone-company-pushed-back-against-nsas-data-collection-court-papers-show.html.

110. Oral Argument, *supra* note 108, at 5–6.

111. *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573, at *2–3 (FISA Ct. Aug. 29, 2013).

112. *Id.* at *2 n.13 ("If a service provider believed that a business records order infringed on its own Fourth Amendment rights, it could raise such a challenge pursuant to 50 U.S.C[.] § 1861(f)."). Though the opinion only references the provider's Fourth Amendment rights, it should be inferred from *Directives* that any cause of action asserted by the provider would include constitutional infringements suffered by its customers. The causes of action set forth in the different statutes are similar. *Compare* 50 U.S.C. § 1861(f)(2)(A)(i) ("A person receiving a production order may challenge the legality of that order by filing a petition . . . ."), *with* Protect America Act of 2007, Pub. L. No. 110-55, § 2, 121 Stat. 552, 554 ("A [service provider] receiving a directive . . . may challenge the legality of that directive . . . ."). Another FISC judge later confirmed this reading, holding that a service provider could assert the Fourth Amendment rights of its customers. *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things, No. BR 14-01, slip op. at 6–9 (FISA Ct. Mar. 20, 2014). However, District Court Judge Rosemary Collyer ruled that the third-party doctrine applied and therefore customers were not entitled to Fourth Amendment protection of their non-content dialing data. *Id.* at 30–31.

113. *In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Redacted]*, 2013 WL 5741573, at *5; *see also* Letter from Judge Walton, *supra* note 109, at 7 (describing *Directives* as the only "instance in which the [FISC] heard arguments from a nongovernmental party that sought to substantively contest a directive from the government"). *But see* Savage, *supra* note 109.

of the corporate avatar dynamic. As discussed in Part IV, there are many reasons to question whether the private company can approximate an individual's relationship to the government. But it is even more problematic to presume that the lack of corporate challenge means that government surveillance is reasonable.

C. STATUTORY ENACTMENT OF THE CORPORATE AVATAR DYNAMIC

Due in part to the third-party doctrine and the resulting lack of Fourth Amendment protection for individual users, Congress has sought to strengthen privacy safeguards without actually requiring a warrant. But these purported protections reflect a statutory embrace of the corporate avatar dynamic. Rather than affording individuals mechanisms to challenge government requests for their information, Congress has empowered the tech company, and sometimes simultaneously precluded individuals from seeking relief.

Two general features of these statutes are: (1) lack of notice to the individual that the government has requested the person's data; and (2) immunity for the tech company's assistance. As is discussed in Part V, without notice, the individual most often with the greatest reason to challenge the surveillance is not even in a position to know whether to challenge. And as is addressed in Part IV, immunity decreases the likelihood that a tech company will oppose government surveillance. The SCA (at issue in *Warshak*) authorizes service providers to turn over the content and non-content information relating to wire or electronic communications in response to government requests.[114] The SCA authorizes the provider's disclosure of communication contents held more than 180 days without a warrant and delay of notice for long periods of time.[115]

The SCA's provisions provide even less protection for individuals' "non-content" data. First, under the SCA, only the service provider has a statutory right to challenge a court order requiring production of non-content data.[116] At least one district court has held that the absence of any provision for a user's challenge evinces congressional intent to restrict such challenges to service providers.[117] Second, the SCA affords immunity to service providers

114. 18 U.S.C. § 2703(a)–(d) (2012); *see also* 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, 1209–24 (2004) (providing a general history and synopsis of the SCA).

115. *See* 18 U.S.C. §§ 2703(b)(1)(B)(i)–(ii), 2703(d), 2705(a)(1)(A)–(B), 2705(a)(4) (allowing for a 90-day delay of notification and for an extension of delays based on a certification of need by a government official); *see also* Kerr, *supra* note 114, at 1233–34.

116. 18 U.S.C. § 2703(d).

117. *In re* Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 128–29 (E.D. Va. 2011). The court inferred the preclusion of a customer challenge in light of the explicit provision in section 2704(b) for customer challenges to orders requiring service providers to create backup copies of electronic communications. *See id.* at 129; *see also In re*

that comply with government requests made pursuant to the statute.[118] Finally, the government is not required to provide notice to users.[119]

Moreover, the SCA authorizes administrative subpoenas or National Security Letters ("NSLs") requiring service providers to turn over the "name, address, length of service, and local and long distance toll billing records of a person or entity" based solely on various Federal Bureau of Investigation ("FBI") officials' certification that the information is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities."[120] No judicial approval is required. The FBI can also require the service provider to not disclose the request to anyone on the basis of national security and other concerns.[121] Congress has, however, permitted service providers the right to "petition for an order modifying or setting aside the request."[122]

The "Pen Registers and Trap and Trace Devices" Statute[123] provides that the government may obtain court orders authorizing the installation of pen registers and traps on phone communications based upon a showing that "information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[124] Lack of notice and disincentives for the tech company to challenge a pen register or a trace also distinguish the statute. The statute also prohibits disclosure of surveillance, authorizes compensation for providers' expenses incurred in cooperating, prohibits any causes of action against third parties providing assistance, and establishes a good faith reliance defense.[125]

FISA establishes a framework for foreign intelligence surveillance and collection that is distinct from the domestic criminal justice sphere.[126] Under FISA, a separate court (the FISC) may grant surveillance requests based on a lesser showing than the Fourth Amendment's warrant requirement.[127] FISA

Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Redacted], 2013 WL 5741573, at *5 (comparing section 215 orders to § 2703(d) orders).

118. 18 U.S.C. § 2703(e); *see also id.* § 2707(e) (providing a good faith reliance defense to civil and criminal actions).

119. *Id.* § 2703(c)(3).

120. *Id.* § 2709(b)(1); *see also id.* § 2703(c)(2). In addition to the SCA, four other statutes authorize NSLs. *See* 12 U.S.C. § 3414(a)(5) (2012) (covering records of financial institutions); 15 U.S.C. §§ 1681u, 1681v (2012) (covering credit reports); 50 U.S.C. § 436 (2012) (covering records relating to the finances and travel of government employees in connection with classified information leak investigations).

121. 18 U.S.C. § 2709(c)(1).

122. *Id.* § 3511(a).

123. *Id.* §§ 3121–3127.

124. *Id.* § 3122(b)(2). Orders for the installation of pen registers and trap devices are limited to 60 days but may be extended for additional 60-day periods. *Id.* § 3123(c).

125. *Id.* §§ 3123(d), 3124(c)–(e).

126. 50 U.S.C. §§ 1801–1885c.

127. *Id.* §§ 1802–1805; s*ee also In re*: Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002) (upholding FISA against a Fourth Amendment challenge).

requires the government to show probable cause only that the electronic surveillance target is a foreign power or an agent of a foreign power.[128] The statute further authorizes the Attorney General to direct common communications carriers to "furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers."[129] The carrier is also compensated for its assistance.[130]

But section 702 of FISA (at issue in *Amnesty International*) removes the general FISA "foreign power" or "agent of foreign power" requirement. Section 702 authorizes the Attorney General and the Director of National Intelligence to jointly authorize "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information," subject to FISC approval.[131] The section provides that the entity receiving a production order may file a petition to challenge such production.[132] But the government may direct the electronic communications provider to assist in the surveillance in a secretive and nonintrusive manner.[133] And the statute authorizes compensation for the provider's assistance[134] and immunizes the provider for its compliance.[135]

Section 215 of the USA PATRIOT Act—the government's basis for its bulk telephony metadata collection—provides that a person receiving an order of production may file a petition to challenge such production.[136] However, lower courts addressing section 215 challenges have held that only the recipient (i.e., not the user or customer target of the order) can challenge the order, with the exception of constitutional claims.[137] Strict limitations prohibit the recipient from disclosing the order to anyone.[138] The statute also immunizes anyone who complies with the order.[139] Thus, a constitutional challenge by the individual user or customer is only possible through unauthorized leaks.[140]

128. 50 U.S.C. § 1805(a)(2)(A)–(B).

129. *Id.* § 1802(a)(4)(A).

130. *Id.* § 1802(a)(4)(B).

131. *Id.* § 1881a(a).

132. *Id.* § 1881a(h)(4)(A); *see also* Letter from Judge Walton, *supra* note 109, at 8. Rule 19(a) of the FISC Rules of Procedure also may facilitate judicial review by authorizing government motions for contempt or sanctions based on a party's noncompliance with a court order. *Id.*

133. 50 U.S.C. § 1881a(h)(1)(A).

134. *Id.* § 1881a(h)(2).

135. *Id.* § 1881a(h)(3).

136. *Id.* § 1861(f)(2)(A)(i); Letter from Judge Walton, *supra* note 109, at 8.

137. *See, e.g.*, Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 740–42 (S.D.N.Y. 2013); Klayman v. Obama, 957 F. Supp. 2d 1, 22–25 (D.D.C. 2013).

138. 50 U.S.C. § 1861(d)(1).

139. *Id.* § 1861(e).

140. *Am. Civil Liberties Union*, 959 F. Supp. 2d at 742.

The upshot of these statutes is that the third-party corporation is granted a means to challenge government requests for information relating to their users. However, under these statutes, the individual is not notified of the information collection or the surveillance and the service provider is statutorily incentivized to assist the government.

IV. THE LIMITS OF THE CORPORATE AVATAR DYNAMIC

The corporate avatar dynamic has been unsuccessful in at least two ways. First, the vast numbers of government requests for user data and the corresponding high compliance rate by companies indicate that corporations do not usually contest the requests. This compliance affects hundreds of thousands of individuals. Second, the records and judicial opinions from the few times when tech companies did challenge the government's requests demonstrate that tech companies are not likely to make effective arguments on behalf of users. In short, they are not good avatars.

A. CORPORATE AVATAR CHALLENGES

Usually when the U.S. government requests user data from Internet companies, the companies provide data. Tech companies' own reports support Justice Ginsburg's incredulity that companies will normally oppose government requests for user information.[141] Though we cannot know the exact number of instances that companies actively oppose government requests,[142] the reports belie the suggestion that companies are effective surrogates for their users.[143]

Examining Google's response to the government's requests illustrates the fallacy of the corporate avatar dynamic.[144] As with a number of Internet

141. *See supra* text accompanying notes 108–10.

142. *See* NATE CARDOZO ET AL., ELEC. FRONTIER FOUND., WHO HAS YOUR BACK? WHICH COMPANIES HELP PROTECT YOUR DATA FROM THE GOVERNMENT? THE ELECTRONIC FRONTIER FOUNDATION'S THIRD ANNUAL REPORT ON ONLINE SERVICE PROVIDERS' PRIVACY AND TRANSPARENCY PRACTICES REGARDING GOVERNMENT ACCESS TO USER DATA 13 (2013), *available at* https://www.eff.org/sites/default/files/who-has-your-back-2013-report-20130513.pdf (noting that secrecy requirements and informal challenges help explain the limited record of companies challenging the government); Miller, *supra* note 90 (reporting that tech companies may initially push back against national security requests for customer information and seek modification of requests even if they ultimately provide information, rather than pursue litigation).

143. It may be fairly asked what percentage of requests a tech company must challenge in order to consider it a reliable surrogate or avatar. While a specific number may prove elusive, it is reasonable to expect that a purported guardian of a user's privacy might object to requests for the person's data more often than not. That proposition suggests that a reliable corporate avatar should challenge requests for users' data more than 50% of the time.

144. Google is the most useful and important Internet company example, due to its dominance of the Internet. By one measure, Google accounts for nearly 25% of all Internet traffic. Craig Labovitz, *Google Sets New Internet Record*, DEEPFIELD (July 22, 2013), http://www.deepfield.net/2013/07/google-sets-new-Internet-record; *see also* VAIDHYANATHAN, *supra* note 35, at 14 ("[N]o single state, firm, or institution in the world has as much power over Web-based

companies, Google produces a Transparency Report, which documents government requests for user data and its compliance.[145]

In the first half of 2014, Google received 12,539 user data requests, specifying 21,576 users, from U.S. law enforcement agencies. Google produced data in response to 84% of the requests.[146] In all of 2013, U.S. law enforcement made 21,492 user data requests to Google, specifying 39,937 users. Google provided data 83% of the time.[147]

In national security and intelligence-related matters, it is more difficult to parse the government's requests for user information and Google's compliance rate. Since 2003, the government has made hundreds of thousands of NSL requests.[148] In 2014, the Department of Justice reported that the FBI had made 14,219 NSL requests (excluding those made solely for subscriber information) relating "to 5334 United States persons."[149] Google is only permitted to report a range of the NSLs it received, stating that for the first half of 2014, it received between 0 and 999 NSLs specifying between 0 and 999 users or accounts.[150] In the second half of 2013, the government issued between 0 and 999 NSLs to Google concerning 1000 and 1999 users or accounts.[151]

Under the FISA regime, companies comply nearly 100% of the time with government directives and orders. In fact, only one time—when Yahoo!

activity as Google does."). Google suggests that the total number of users specified could be "over-inclusive" because different data requests may include the same user or account. *Transparency Report: FAQ*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/faq/ (last visited Mar. 7, 2015).

145. *See* CARDOZO ET AL., *supra* note 142, at 11.

146. *Transparency Report: Countries (January to June 2014)*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/countries/?p=2014-06 (last visited Mar. 7, 2015) (noting the data also include requests for information at YouTube). The compliance rate reflects both complete and partial accommodation of government requests. *Id.* According to Google, "[w]e review each request to make sure that it complies with both the spirit and the letter of the law, and we may refuse to produce information or try to narrow the request in some cases." *Id.*

147. *Transparency Report: Countries (January to June 2013)*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/countries/?p=2013-06 (last visited Mar. 7, 2015) (including YouTube data); *Transparency Report: Countries (July to December 2013)*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/countries/?p=2013-12 (last visited Mar. 7, 2015) (including YouTube data).

148. *See, e.g.*, Dan Eggen, *FBI Found to Misuse Security Letters*, WASH. POST (Mar. 14, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/03/13/AR2008031302277.html (citing Justice Department Inspector General Glen Fine's finding that the FBI issued nearly 200,000 national security letters between 2003 and 2006).

149. Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney Gen., to Senator Harry Reid, Senate Majority Leader 2 (Apr. 30, 2014) [hereinafter Letter from Peter J. Kadzik], *available at* http://fas.org/irp/agency/doj/fisa/2013rept.pdf.

150. *Transparency Report: Overview (United States)*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/US/ (last visited Mar. 7, 2015).

151. *Id.*

refused to comply with a directive—has a recipient failed to accede to a FISA production order.[152]

FISA order recipients' near-total compliance raises concerns, given the thousands of secretive requests that have been made. From 1979 through 2013, the government made 35,333 applications to the FISC to conduct electronic surveillance and physical searches for foreign intelligence purposes.[153] Over these 34 years, the FISC disapproved just 12 requests for collection authority.[154] In 2013, the FISC approved all 1588 applications for authority to conduct electronic surveillance.[155] Similarly, the FISC did not deny any of the 178 applications for business records and tangible things under section 215 of FISA.[156]

As with NSLs, Google may only report the range of FISA requests it has received. Dating back to 2009, Google reports it has received 0 to 999 requests for non-content data under FISA for 0 to 999 users or accounts every six-month period.[157] The government has, however, sought content data concerning far more users or accounts.[158] For example, Google reports that in the second half of 2013, the government made 0 to 999 requests for content data under FISA regarding 15,000 to 15,999 users or accounts.[159] In the preceding six-month period, the government sought content data for 9000 to 9999 users or accounts.[160]

Other Internet companies' reports also reveal tens of thousands of government requests for data and—where the companies have disclosed—high rates of cooperation. According to Facebook's own self-reporting, during

152. Letter from Judge Walton, *supra* note 109, at 7; *see also supra* Part III.B (discussing *Directives*). Judge Walton also noted that the FISCR accepted amici curiae briefs from the American Civil Liberties Union and the National Association of Criminal Defense Lawyers in *In re: Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002). *See* Letter from Judge Walton, *supra* note 109, at 8 n.10.

153. *Foreign Intelligence Surveillance Act Court Orders 1979–2014*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/wiretap/stats/fisa_stats.html (last visited Mar. 7, 2015).

154. *Id.*

155. *See* Letter from Peter J. Kadzik, *supra* note 149, at 1. The government notes in its report that the FISC modified 36 proposed orders. *Id.* at 1–2 & n.1. FISA defenders argue that applications and requested orders undergo significant changes through the FISC process. Letter from the Honorable Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to Senator Charles E. Grassley, Ranking Member, Senate Comm. on the Judiciary 1 (Oct. 11, 2013), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/10/ranking-member-grassley-letter-131011.pdf.

156. Letter from Peter J. Kadzik, *supra* note 149, at 2. The FISC did modify 141 of the proposed section 215 orders. *Id.*

157. *Transparency Report: Overview (United States)*, *supra* note 150. Google defines "non-content information" as "the same kind of information that can be requested under a criminal subpoena or criminal order under the Electronic Communications Privacy Act." *Id.*

158. *Id.* Google defines "private content" as "the same kind of information that can be requested under a criminal search warrant or wiretap order." *Id.*

159. *Id.*

160. *Id.*

the second half of 2013 it received 12,598 U.S. law enforcement requests for user data, affecting 18,715 accounts.[161] Facebook complied with 81.02% of these requests.[162]

Phone companies appear to be even worse corporate avatars. For example, AT&T received 115,925 U.S. criminal and civil litigation demands in the first half of 2014.[163] The company rejected or challenged 2110, or 1.8%, of these demands.[164] In the same time period, AT&T also received 1000 to 1999 NSLs concerning 2000 to 2999 customer accounts; 0 to 999 content requests under FISA pertaining to 33,000 to 33,999 accounts; and 0 to 999 requests for non-content data about 0 to 999 accounts.[165] Similarly, Verizon reports that in the first half of 2014 it received 148,903 U.S. law enforcement demands for customer data.[166] Of these requests, the government sought 72,342 subpoenas, 14,977 warrants, and 37,327 orders for user data.[167]

161. *Government Requests Report: United States (July 2013–December 2013)*, FACEBOOK, https://govtrequests.facebook.com/country/United%20States/2013-H2 (last visited Mar. 7, 2015).

162. *Id.* In the second half of 2013, Facebook also received 0 to 999 FISA content requests concerning 5000 to 5999 users or accounts; 0 to 999 FISA non-content requests for 0 to 999 users or accounts; and 0 to 999 NSLs about 0 to 999 users or accounts. *Id.* Of course, rates of compliance and the substance of the information provided vary with Internet companies. Microsoft reports that in the first half of 2014, it received 6919 user data requests and 15,730 users specified from U.S. law enforcement agencies. *Corporate Citizenship: Law Enforcement Requests Report*, MICROSOFT, http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency (last visited Mar. 7, 2015) (click "2014 (JAN–JUN)," then click the "United States" tile below). Microsoft data include all its services, including Skype. *Id.* (click "Which Microsoft Services are included in this report?"). Of these requests, Microsoft rejected 13.4%; lacked data for 14%; provided transactional or subscriber data for 62.5%; and disclosed content data for 10.1%. *Id.* Microsoft also reports that in the second half of 2013, it received 0 to 999 orders under FISA seeking content, impacting 18,000 to 18,999 accounts; 0 to 999 orders under FISA seeking non-content data, affecting 0 to 999 accounts; and 0 to 999 NSLs about 0 to 999 accounts. *Corporate Citizenship: U.S. National Security Orders Report*, MICROSOFT, http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/fisa/ (last visited Mar. 7, 2015). Twitter, by comparison, reports that in the first half of 2014, it received 1257 data requests pertaining to 1918 specific accounts, to which the company provided some information 72% of the time. *Transparency Report: United States*, TWITTER, https://transparency.twitter.com/country/us (last visited Mar. 7, 2015). Twitter distinguished itself in its reporting of notice to the user. Twitter states that in the first six months of 2014, it gave notice to users about 6% of U.S. law enforcement's information requests. *Id.* Twitter also reports that 11% of requests were under seal, precluding notice. *Id.* No notice was provided 83% of the time, despite the lack of a seal. *Id.*

163. AT&T INC., AT&T TRANSPARENCY REPORT 3 (2014), *available at* http://about.att.com/content/dam/csr/PDFs/ATT_Transparency%20Report_July%202014.pdf. From AT&T's own data, it appears that civil litigation demands comprise 7968 subpoenas. *Id.*

164. *Id.* at 4. In addition to the rejections and challenges, AT&T reports that it provided either only partial or no information in response to 28,987 demands. *Id.*

165. *Id.* at 3.

166. VERIZON, VERIZON'S TRANSPARENCY REPORT FOR THE FIRST HALF OF 2014: UNITED STATES REPORT 1 (2014), *available at* http://transparency.verizon.com/themes/site_themes/transparency/archive/Verizon-Transparency-Report-2014-first-half.pdf.

167. *Id.*

Verizon refused to comply with approximately 3% of the subpoenas and approximately 4.5% of the orders and warrants.[168]

B. THE PROBLEM OF NONDISCLOSURE

The tech companies' transparency reports achieve their eponymous objective at only the most general level.[169] Frequently, the companies do not tell their users about the government surveillance specific to them. Google explains in its Transparency Report that it notifies users about legal demands, unless prohibited by law or court order.[170] Google asserts that "[i]n certain cases" it will "push back regardless of whether the user decides to challenge [a request] legally."[171] But when Google will fight limits on disclosure is not clear from its report.[172] In addition, as Google acknowledges, FISA request

168. *Id.*

169. Tech companies' transparency reports reveal more data than had been previously permitted by the United States government. Earlier reports had not been permitted to include even ranges of FISA and NSL requests. Litigation efforts by Google, Microsoft, Facebook, Yahoo!, and Linkedin precipitated a settlement with the government allowing publication of more data. *See* Motion for Declaratory Judgment of Google Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders at 4, *In re* Motion for Declaratory Judgment of Google Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders, No. Misc. 13-03 (FISA Ct. June 18, 2013); Letter from James M. Cole, Deputy Attorney Gen., to Colin Stretch, Vice President and Gen. Counsel, Facebook, et al. 1–2 (Jan. 27, 2014), *available at* http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf (stating that the "letter memorializes additional ways in which the government will permit [tech companies] to report data concerning requests for customer information," specifically including the publication, albeit in aggregate form, of FISA orders and NSLs). Twitter, however, has sued the United States government over the continuing limitations on data concerning NSLs and FISA-related orders. *See* Complaint for Declaratory Judgment, 28 U.S.C. §§ 2201 and 2202, Twitter, Inc. v. Holder, No. 14-cv-4480 (N.D. Cal. Oct. 7, 2014). Twitter claims the limitations amount to a violation of the First Amendment and seeks to report smaller ranges of data requests, whether zero requests were made, and additional descriptive details. *Id.* at 11–12.

170. *Transparency Report: Legal Process*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/legalprocess/ (last visited Mar. 7, 2015).

171. *Id.*

172. A prior iteration of Google's explanation to users concerning notice indicated it would only provide notice "when appropriate" and that it would "sometimes fight" government data requests. *See* CARDOZO ET AL., *supra* note 142, at 10–11 (criticizing Google for "ambiguity" of policy and noting that some Internet companies' policies, including those of Twitter and LinkedIn, are less equivocal in their commitment to notifying users of government data requests); Shara Tibken, *Google: Here's How We Handle Government Requests About You*, CNET (Jan. 28, 2013, 8:19 AM), http://www.cnet.com/news/google-heres-how-we-handle-government-requests-about-you ("We sometimes fight to give users notice of a data request by seeking to lift gag orders or unseal search warrants." (quoting Google's earlier transparency policy) (internal quotation marks omitted)). Even Twitter, an Internet company long praised for its users' privacy protection, reports that it only gives users notice of government requests for data 6% of the time, despite 89% of these requests having not been made "under seal." *Transparency Report: United States*, *supra* note 162; *see also supra* note 162.

recipients cannot disclose even the fact of the demand, and the government can prohibit the disclosure of NSLs quite easily.[173]

Orin Kerr observes that third-party businesses may assert their users' First Amendment rights in challenging NSLs.[174] ISPs certainly *may* assert their customer's rights when the interests of users and providers coincide. But very rarely does a communications service provider *actually* challenge the nondisclosure requirement.

Notwithstanding the free speech interest of third-party businesses, "[t]he typical NSL recipient . . . has little if any incentive to initiate a court challenge in order to speak publicly about such receipt."[175] The United States Court of Appeals for the Second Circuit observed that although there were 40,000 NSL requests issued in 2005, "perhaps no more than three" service providers challenged the nondisclosure requirement.[176]

Based in part on how infrequently providers actually challenge requests, the Second Circuit fashioned an alternative judicial review mechanism for the nondisclosure requirement. Instead of mandating that the government initiate judicial review of all nondisclosure orders, the court construed the statute to require the government to just inform the provider that it can contest the nondisclosure, and if there is opposition, the government would be required to seek judicial review.[177] In response to the decision, the Justice

173. *Transparency Report: FAQ*, *supra* note 144.

174. Kerr, *supra* note 4, at 599–600 (discussing Doe v. Gonzales, 500 F. Supp. 2d 379 (S.D.N.Y. 2007), *aff'd in part, rev'd in part, remanded by* John Doe, Inc. v. Mukasey, 549 F.3d 861 (2d Cir. 2008)).

175. *John Doe, Inc.*, 549 F.3d at 880. The process is very difficult and highly secretive for an NSL recipient. For a good description of the NSL process from a recipient's perspective, see Maria Bustillos, *What It's Like to Get a National-Security Letter*, NEW YORKER (June 27, 2013), http://www.newyorker.com/tech/elements/what-its-like-to-get-a-national-security-letter.

176. *John Doe, Inc.*, 549 F.3d at 879. There are few other cases documenting service providers' challenges to the government's gag orders on NSLs. *See, e.g.*, *In re* Nat'l Sec. Letter, 930 F. Supp. 2d 1064, 1074 (N.D. Cal. 2013)("[D]espite evidence demonstrating that tens of thousands of NSLs are issued each year—and by the government's own estimate, 97% of them may come with a nondisclosure order—only a handful of challenges to the NSL provisions have been brought."); *id.* at 1074 n.12 (referring to a challenge of a nondisclosure order in 2012 in the Eastern District of Virginia but noting "the NSL recipient did not appear in Court or otherwise participate"); Doe v. Gonzales, 386 F. Supp. 2d 66, 82 (D. Conn. 2005); Doe v. Ashcroft, 334 F. Supp. 2d 471, 506 (S.D.N.Y. 2004), *vacated in part by* Doe v. Gonzales, 449 F.3d 415, 419 (2d Cir. 2006); *see also In re* Nat'l Sec. Letters, No. C-13-80063 SI, slip op. at 2–4 (N.D. Cal. May 20, 2013); Declan McCullagh, *Justice Department Tries to Force Google to Hand Over User Data*, CNET (May 31, 2013, 9:21 AM), www.cnet.com/news/justice-department-tries-to-force-google-to-hand-over-user-data/ (describing Google's and the Electronic Frontier Foundation's challenges against NSLs on behalf of service providers).

177. *John Doe, Inc.*, 549 F.3d at 883–84.

Department requires that all NSLs inform recipients that they may challenge the gag order "through the government initiated judicial review."[178]

Although this solution empowers the service provider, it does not support separation-of-powers principles.[179] Judicial review occurs only if the provider objects to the NSL. Thus, the service provider is the primary check on Executive branch overreaching, and its interests in disclosure are not clear and may not coincide with users.

C. CORPORATE AVATAR ARGUMENTS

Gonzales v. Google, Inc. is the paradigmatic case of an ISP's successfully fighting a government request for user data.[180] It is frequently cited to praise Google's concern for user interests and to support a tech company's ability to fight for user rights and limit government searches.[181] But in addition to being something of an outlier, Google's arguments in the case call into question the adequacy of the corporate avatar's representation of an individual's interests.

To obtain information about filtering and blocking software that was related to litigation over the constitutionality of the Child Online Protection Act, the government subpoenaed several search engines' search query records and a listing of URLs available to their users.[182] Google, unlike the other companies, contested the subpoenas, which initially sought *all* URLs available for search requests and *all* users' queries entered on Google for a two-month period.[183] Google argued that the information was not relevant and that producing the data was an undue burden.[184]

But beyond asserting that "[t]he privacy of Google users matters," Google only addressed the disclosure's effect on its business and consumer confidence.[185] Google argued that if compelled to produce the data, it would

178. Letter from Eric H. Holder, Jr., U.S. Attorney Gen., to Senator Patrick J. Leahy, Chairman, U.S. Senate Comm. on the Judiciary 2 (Dec. 9, 2010), *available at* http://www.wired.com/images_blogs/threatlevel/2012/05/letter_to_patrick_leahy_2010.12.09.pdf.

179. *See In re Nat'l Sec. Letter*, 930 F. Supp. 2d at 1081 (holding that "the nondisclosure provision of 18 U.S.C. § 2709(c) violates the First Amendment and" that the limited scope of judicial review under "18 U.S.C. § 3511(b)(2) and (b)(3) violate[s] the First Amendment and separation of powers principles").

180. Gonzales v. Google, Inc., 234 F.R.D. 674 (N.D. Cal. 2006).

181. *See, e.g.*, Kerr, *supra* note 4, at 599; *Transparency Report: Legal Process*, *supra* note 170 ("For example, in 2006 Google was the only major search company that refused a U.S. government request to hand over two months' [sic] of user search queries. We objected to the subpoena, and eventually a court denied the government's request.").

182. *Gonzales*, 234 F.R.D. at 678–79.

183. *Id.* at 679. Google first negotiated the government requests down to 50,000 URLs and 5000 search entries, but still objected to these reduced demands. *Id.*

184. *Id.* at 682–83.

185. Google's Opposition to the Government's Motion to Compel at 2, 19, *Gonzales*, 234 F.R.D. 674 (No. 5:06-mc-80006-JW), 2006 WL 543697.

"suffer a loss of trust among users," and that users would "be less likely to use the service."[186]

The district court appreciated that Google's privacy arguments did not extend to Google users. On its own, the court considered Google users' privacy interests as distinct "from Google's business goodwill argument."[187] The court suggested users' search queries could reveal particular sensitive information, a concern that, the court noted, was not raised by Google or the government.[188]

Ultimately, the court did not rule on the potential customer privacy rights violations because it determined the search query information was duplicative and could harm Google users' trust.[189] The court therefore granted the government's motion to compel production, but only as to the URLs.

If *Google, Inc.* is the lodestar case for the corporate avatar dynamic, then there is ample reason to worry. First, despite Google's opposition, Yahoo!, AOL, and Microsoft acceded to the government requests for data.[190] Thus, the case doesn't represent what most tech companies do in response to government demands for user data. Internet companies' own records on compliance with government data requests demonstrate how truly exceptional a case like *Google, Inc.* is.[191] As a result, the case offers minimal support for the proposition that third parties will protect their customers' privacy interests or sufficiently challenge government excess.

Second, how a party makes its arguments and what it argues matters. Google's failure to effectively assert its customers' privacy rights raises questions about service providers' interest, commitment, and ability to effectively challenge government searches. Though Google's arguments invoked customer privacy, the arguments were framed in terms of perceptions about Google and loss of goodwill—it was focused on the injury to Google, rather than to the users—a perhaps less sympathetic framing than the users' own violation or loss of privacy.[192]

That Google did not muster a more aggressive privacy argument may also be understandable given the search engine's business.[193] Arguing an aggressive or expansive form of customer privacy would also have been against Google's own business interests. The more expansive a conception of privacy

186. *Id.* at 18; *see also Gonzales*, 234 F.R.D at 684–85.

187. *Gonzales*, 234 F.R.D. at 687.

188. *Id.* For example, the court noted, a user might enter a search query for "[user name] third trimester abortion san jose." *Id.*

189. *Id.* at 686, 688.

190. *Id.* at 679.

191. *See supra* Part IV.A.

192. *See* VAIDHYANATHAN, *supra* note 35, at 87 (contending that Google opposed the government's demands "not to protect its users' privacy but to protect its trade secrets").

193. *See infra* Part V.A.4 (discussing Internet companies' attitudes toward user privacy).

from disclosure to other parties of information supplied to Google, the more limited Google might be in providing customer information to not only the government, but to other commercial entities, such as advertisers, which is the primary source of revenue for Google.[194]

While the court made findings about users' privacy sua sponte, the lack of a true customer advocate is problematic. An advocate is likely to marshal more aggressive arguments than may a neutral decisionmaker. Google and other third-party businesses cannot be expected to assert the rights of their customers. Indeed, in many cases, there is even a conflict of interest, as it would seem there was here. Although Google did challenge the government and limited the scope and substance of information it had to produce, that Google did not actually assert the rights of its customers is significant. In other cases, the lack of that advocacy may impact the judge in upholding or denying government requests for customer information. At the very least, Google's limited assertion of customer rights, together with other Internet companies' acquiescence, raises doubts about whether government overreach may be deterred by corporations' lawyers.[195]

Other service providers have of course challenged government requests for user data as well. But the mixed results and efforts evidence the limits of vesting privacy protection in corporations.[196] Though Yahoo! succeeded in securing the right to bring a "Fourth Amendment claim on behalf of its customers," the FISCR upheld the government's warrantless surveillance directives.[197] The court held in *Directives* "that a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States."[198] The court characterized the government interest in national security to be "of the highest order of magnitude," and dismissed Yahoo!'s concerns as a "parade of horribles," without "evidence of any actual harm, any egregious risk of error, or any broad potential for abuse in the circumstances of the instant case."[199] The government's national security interest may have been insurmountable but,

194. *See* Ryan Singel, *How Does Google Make the Big Bucks? An Infographic Answer*, WIRED (July 19, 2011, 10:44 AM), http://www.wired.com/2011/07/google-revenue-sources.

195. *Cf.* Kerr, *supra* note 4, at 600.

196. Twitter has distinguished itself as perhaps the most aggressive advocate for its users' privacy, but these efforts have met limited success. *See, e.g.*, Russ Buettner, *A Brooklyn Protester Pleads Guilty After His Twitter Posts Sink His Cas*e, N.Y. TIMES (Dec. 12, 2012), http://www.nytimes.com/2012/12/13/nyregion/malcolm-harris-pleads-guilty-over-2011-march.html (describing Twitter's efforts to quash a subpoena requiring the production of a user's old and deleted tweets and the company's ultimate compliance).

197. *In re* Directives [Redacted] Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1009 (FISA Ct. Rev. 2008).

198. *Id.* at 1012.

199. *Id.* at 1012–13.

as a corporate entity, it was doubtless more difficult for Yahoo!, than for a person, to convince a court of actual harm and rise above theoretical wrongs.[200]

Service providers have also argued since at least 2004 that warrants were required for government requests for email contents.[201] But service providers' concerns about uniformity of policy and limiting their own liability may have motivated these arguments more than protecting their users' privacy.

In *United States v. Weaver*, for example, the government subpoenaed a defendant child pornographer's MSN/Hotmail email contents.[202] Microsoft refused to produce previously opened emails less than 181 days old.[203] But rather than directly respond to the government's motion to compel compliance with the subpoena, Microsoft wrote a one-page letter, asking only that the government include it with the motion to compel. Microsoft simply stated that the Ninth Circuit's opinion in *Theofel v. Farey-Jones* required a warrant, and the opinion applied because Microsoft is headquartered within the Ninth Circuit and compliance with the subpoena would occur there.[204] Microsoft explained that "the Ninth Circuit has deemed opened email to be in electronic storage for backup preservation" and therefore, required a warrant per the SCA.[205] The district court was unpersuaded by Microsoft's arguments, however, and ordered Microsoft to comply with the subpoena.[206]

200. *See id.* at 1008. Yahoo!'s efforts deserve plaudits. Yahoo!'s resolute pursuit of its challenge on behalf of its users was made under threat of civil contempt fines of $250,000 per day. Vindu Goel & Charlie Savage, *Government's Threat of Daily Fine for Yahoo Shows Aggressive Push for Data*, N.Y. TIMES (Sept. 11, 2014), http://www.nytimes.com/2014/09/12/technology/documents-unsealed-in-yahoos-case-against-us-data-requests.html. It also appears that only Yahoo!, among seven other companies receiving surveillance requests, challenged the government. *See id.* Many of the documents related to the litigation have been declassified thanks to Yahoo!'s efforts and are available for viewing. *See* Office of the Dir. of Nat'l Intelligence, *Statement by the Office of the Director of National Intelligence and the U.S. Department of Justice on the Declassification of Documents Related to the Protect America Act Litigation*, IC ON THE RECORD (Sept. 11, 2014), http://icontherecord.tumblr.com/post/97251906083/statement-by-the-office-of-the-director-of.

201. *See, e.g.*, United States v. Weaver, 636 F. Supp. 2d 769, 769 (C.D. Ill. 2009); Yahoo! Inc.'s Response to the United States' Motion to Compel Compliance with This Court's 2703(d) Order at 1, *In re* Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), No. Misc. 09-Y-080-CBS (D. Colo. Apr. 13, 2010).

202. *Weaver*, 636 F. Supp. 2d at 769.

203. *Id.* at 770.

204. *Id.* at 770–72 (analyzing Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2003)); Letter from Richard Sauer, Assoc. Gen. Counsel, Microsoft, to Elly N. Pierson, Assistant U.S. Attorney (June 18, 2009) [hereinafter Letter from Richard Sauer], *available at* http://ia601406.us.archive.org/34/items/gov.uscourts.ilcd.46490/gov.uscourts.ilcd.46490.12.1.pdf (marked as "Exhibit 2"); *see also* Dan Sachs, *Another Federal Court Rules That Opened Emails Are Not in "Electronic Storage" Under the Stored Communications Act*, ZWILLGEN BLOG (June 20, 2013), http://blog.zwillgen.com/2013/06/20/another-federal-court-rules-that-opened-emails-are-not-in-electronic-storage-under-the-stored-communications-act ("Because many national service providers are based in the Ninth Circuit, *Theofel* has effectively been the law of the land for many years.").

205. Letter from Richard Sauer, *supra* note 204; *see also Weaver*, 636 F. Supp. 2d at 771.

206. *Weaver*, 636 F. Supp. 2d at 773.

Although arguments pushing for the Ninth Circuit's expansive definition of "electronic storage" in another circuit could redound to users' privacy protection, the short paragraphs in the letter suggest Microsoft may have been primarily concerned with not running afoul of the SCA's limits on disclosure and the company's exposure to liability.[207] Such motivations are unlikely to effectively limit government overreach, particularly where the law immunizes companies from liability for complying with government requests for customer data.

V. THE CORPORATE AVATAR DYNAMIC FALLACY

This Part first explores why the technology industry is unlikely to challenge government requests for user information. But even if tech companies were to challenge government surveillance more frequently and vigorously, their role as the public's avatars presents a normative problem. This Part then examines how the substitution of corporate entities for people controverts the government oversight purposes of the Fourth Amendment and the Framers' skepticism about corporate power.

A. THE CORPORATE AVATAR DYNAMIC'S FUNCTIONAL LIMITATIONS

1. Tech Companies' Relationships with the Government

The government and tech companies enjoy a close, interdependent relationship that is highly beneficial to both sectors.[208] This relationship, which has blossomed since the end of the Cold War, has grown into the "intelligence-industrial complex."[209] In the most practical terms, the government could not conduct any of its electronic surveillance without the private companies providing the instruments and services through which we communicate.[210] The NSA's highest level technology is designed by private

207. *See* 18 U.S.C. §§ 2702(a), 2707 (2012) (setting forth limits on voluntary disclosure and civil action, relief, and damages for improper disclosure); *see also* Yahoo! Inc.'s Response to the United States' Motion to Compel Compliance with This Court's 2703(d) Order, *supra* note 201, at 2 n.1 ("The ruling that the government seeks in this matter would force Yahoo! to either endure a contempt penalty in this court or become vulnerable to civil liability within the Ninth Circuit.").

208. *See, e.g.*, VAIDHYANATHAN, *supra* note 35, at 48–49 (noting Google's "close relationship" with the Obama administration); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1940–41 (2013) (describing the private sector and government surveillance as mutually supportive); Julian Assange, Op-Ed., *The Banality of 'Don't Be Evil,'* N.Y. TIMES (June 1, 2013), http://www.nytimes.com/2013/06/02/opinion/sunday/the-banality-of-googles-dont-be-evil.html (decrying "the ever closer union between the State Department and Silicon Valley").

209. Michael Hirsh, *How America's Top Tech Companies Created the Surveillance State*, NAT'L J. (July 25, 2013), http://www.nationaljournal.com/magazine/how-america-s-top-tech-companies-created-the-surveillance-state-20130725.

210. *See* JAY ROCKEFELLER, SELECT COMM. ON INTELLIGENCE, FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 AMENDMENTS ACT OF 2007, S. REP. NO. 110-209, at 10 (2007); PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 27, at 5–6.

tech companies.[211] There is a virtual revolving door between tech companies and government intelligence and the military.[212] In addition, tech companies store tremendous amounts of our data and have the expertise and capacity to analyze the data.[213]

Private companies also court and serve the government as a client for their electronic communication and big data services. Government agencies contract with tech companies for computing services.[214] These contracts, in particular for cloud computing services, total hundreds of millions of dollars.[215] Google, for example, supplies government agencies with products such as Google Apps that facilitate email and data storage.[216] At least 42,000 federal government employees and contractors use the company's cloud-based email.[217] Similarly, the Central Intelligence Agency has solicited and received bids from various tech companies, including Amazon, Microsoft, and IBM to provide cloud computing services to the intelligence agency.[218] The government also pays out hundreds of millions of dollars to the technology industry for mobile communications devices.[219] Thus, tech companies'

211. Hirsh, *supra* note 209 (noting that government surveillance networks "are virtually interwoven with [tech companies'] products").

212. *See* Rebecca Greenfield, *Facebook's Former Security Chief Now Works for the NSA*, WIRE (June 20, 2013, 9:40 AM), http://www.thewire.com/technology/2013/06/facebooks-former-security-chief-now-works-nsa/66432/; Hirsh, *supra* note 209; Somini Sengupta, *The Pentagon as Silicon Valley's Incubator*, N.Y. TIMES (Aug. 22, 2013), http://www.nytimes.com/2013/08/23/technology/the-pentagon-as-start-up-incubator.html (noting that there are few entities besides the NSA, Facebook, and Google with engineers who have data mining experience).

213. James Risen & Nick Wingfield, *Web's Reach Binds N.S.A. and Silicon Valley Leaders*, N.Y. TIMES (June 19, 2013), http://www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-bound-by-strengthening-web.html.

214. *See, e.g.*, *Apple Store for Government*, APPLE, http://www.apple.com/r/store/government/ (last visited Mar. 9, 2015); *Government*, MICROSOFT, http://www.microsoft.com/government/en-us/Pages/default.aspx (last visited Mar. 9, 2015).

215. *See, e.g.*, J. Nicholas Hoover, *Military Signs Most Comprehensive Microsoft Contract Yet*, INFORMATIONWEEK (Jan. 3, 2013, 10:55 AM), http://www.informationweek.com/government/enterprise-applications/military-signs-most-comprehensive-micros/240145467.

216. *See Google Apps for Government*, GOOGLE, http://www.google.com/enterprise/apps/government/ (last visited Mar. 9, 2015); *Google Government Transformers*, GOOGLE, http://www.govtransformers.com/ (last visited Mar. 9, 2015) (describing various Google products and services used by local governments).

217. *See, e.g.*, Kennith Jackson, *NOAA Moves 25,000 to Google Apps*, OFFICIAL GOOGLE FOR WORK BLOG (Jan. 4, 2012), http://googleenterprise.blogspot.com/2012/01/noaa-moves-25000-to-google-apps.html (stating that 25,000 people are employed at the National Oceanic and Atmospheric Administration); Lance Whitney, *Google Scores Big Federal Government Contract*, CNET (Dec. 2, 2010, 9:07 AM), http://www.cnet.com/news/google-scores-big-federal-government-contract/ (stating that 17,000 people are employed at the U.S. General Services Administration).

218. *See* IBM, B-407073, 2013 WL 2897034, at *1–3 (Comp. Gen. June 6, 2013); Joseph Marks, *Amazon Sues over CIA Cloud Deal*, NEXTGOV (July 29, 2013), http://www.nextgov.com/cloud-computing/2013/07/amazon-sues-over-cia-cloud-deal/67592/.

219. *See, e.g.*, Dara Kerr, *Defense Department Opens Contracts for Apple, Google*, CNET (Feb. 26, 2013, 6:36 PM), http://www.cnet.com/news/defense-department-opens-contracts-for-apple-

extensive and lucrative business relationships with the government may limit their ability to act impartially, let alone act in their users' interests, in responding to government requests and court orders for user information.[220]

In addition, the government regulates private tech companies' services, including, ironically, their compliance with consumer privacy protections.[221] Again, tech companies have a clear interest in appeasing the government in its law enforcement and security interests when they are subject to the government's regulatory arms, such as the Federal Communications Commission and Federal Trade Commission.[222]

2. Government Control over Private Communications Systems

Sharing communications and other customer information with the government is already part of some technologies' DNA. Moreover, laws and security agreements may compel communications service providers to enable their services and products to conduct surveillance at the government's request.

The Communications Assistance for Law Enforcement Act ("CALEA"),[223] for example, requires telecommunications carriers and communications equipment manufacturers to ensure that their products and services permit the government to intercept wire and electronic communications and access call-identifying information.[224] Broadband Internet access and voice over Internet protocol ("VoIP") services are also subject to CALEA.[225] Information services providers, including web-based service providers, are not similarly obligated to modify their services and products to enable government surveillance.[226] But law enforcement has proposed legislation that would

google/ (reporting that the U.S. Defense Department expects to utilize 8,000,000 mobile devices).

220. Hirsh, *supra* note 209 ("[I]t's the good little Indian that gets rewarded. And these companies needed the goodwill of the NSA and other agencies." (quoting an anonymous private-sector official) (internal quotation marks omited)).

221. Tom Risen, *Data Plans, Caps Stoke FCC Net Neutrality Concerns*, U.S. NEWS & WORLD REP. (July 31, 2014, 1:04 PM), http://www.usnews.com/news/articles/2014/07/31/data-plans-caps-stoke-fcc-net-neutrality-concerns. *See generally* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326 privacyreport.pdf.

222. *See generally* FED. TRADE COMM'N, *supra* note 221.

223. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended at 47 U.S.C. §§ 1001–1010 (2012)).

224. *See id.* §§ 1002, 1005.

225. *See* Am. Council on Educ. v. Fed. Commc'ns Comm'n, 451 F.3d 226, 234–35 (D.C. Cir. 2006) (deferring to the FCC decision requiring broadband and VoIP providers to comply with CALEA).

226. *See id.*; *see also* 47 U.S.C. § 1001(6) (defining "information services"); *id.* § 1002(b)(2)(A) (excluding information service providers from CALEA requirements to modify services and product to aid law enforcement).

apply CALEA-like requirements to web-based companies. These requirements range from compelling companies to modify their infrastructure to enable "wiretaps" of emails to a series of escalating fines for noncompliance with government requests.[227]

The NSA has also enjoyed access to tech companies' encryption technologies, approving their export only when the NSA is permitted to both review the technologies and have a "back door" to the data it wanted.[228] Tech companies also may opt to change their code and architecture to facilitate government surveillance, rather than have the government impose its own devices or changes to code and architecture.[229]

Lessig has warned that CALEA and similar government efforts "induce the development of an architecture that makes behavior more regulable."[230] The interdependent relationship of commerce and government, Lessig argues, allows the government to exploit tech companies' financial interests, forcing changes in the Internet's architecture that are not in individual users' interests.[231] Indeed, once the technological infrastructure enables government surveillance, there is less reason for companies to fight a data request. Without a practical impediment and the concomitant costs associated

227. *See* Declan McCullagh, *FBI: We Need Wiretap-Ready Web Sites—Now*, CNET (May 4, 2012, 9:24 AM), http://www.cnet.com/news/fbi-we-need-wiretap-ready-web-sites-now; Ellen Nakashima, *Proposal Seeks to Fine Tech Companies for Noncompliance with Wiretap Orders*, WASH. POST (Apr. 28, 2013), http://www.washingtonpost.com/world/national-security/proposal-seeks-to-fine-tech-companies-for-noncompliance-with-wiretap-orders/2013/04/28/29e7d9d8-a83c-11e2-b029-8fb7e977ef71_story.html; *see also* BEN ADIDA ET AL., CALEA II: RISKS OF WIRETAP MODIFICATIONS TO ENDPOINTS 2, 4–7 (2013), *available at* https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf (criticizing proposed legislation).

228. Hirsh, *supra* note 209; *see also* Shane Harris, *Google's Secret NSA Alliance: The Terrifying Deals Between Silicon Valley and the Security State*, SALON (Nov. 16, 2014, 5:58 AM), http://www.salon.com/2014/11/16/googles_secret_nsa_alliance_the_terrifying_deals_between_silicon_valley_and_the_security_state/ (describing NSA partnerships with tech companies that include the corporate disclosure of weaknesses and back doors to the agency in order to improve their security against cyber attacks); David E. Sanger & Claire Cain Miller, *In Keeping Grip on Data Pipeline, Obama Does Little to Reassure Industry*, N.Y. TIMES (Jan. 17, 2014), http://www.nytimes.com/2014/01/18/technology/in-keeping-grip-on-data-pipeline-obama-does-little-to-reassure-industry.html (noting the government paid RSA, an encryption firm, to include an inferior algorithm in its products in order to facilitate "back door" access for the NSA); Craig Timberg, *Police Want Back Doors in Smartphones, but You Never Know Who Else Will Open Them*, WASH. POST (Oct. 2, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/02/police-want-back-doors-in-smartphones-but-you-never-know-who-else-will-open-them/ (describing security experts' general criticism of back doors and the government's concerns about Apple's and Google's encryption of their devices).

229. *See* Declan McCullagh, *How the U.S. Forces Net Firms to Cooperate on Surveillance*, CNET (July 12, 2013, 12:30 PM), http://www.cnet.com/news/how-the-u-s-forces-net-firms-to-cooperate-on-surveillance (describing Microsoft's decision to design a system allowing for cooperation with government requests in order to avoid the government's implanting of a surveillance device in its internal system).

230. LESSIG, *supra* note 7, at 62.

231. *Id.* at 77–80.

with overcoming logistical hurdles to provide the data, technological companies will have fewer reasons to resist government requests.

3. The Private Tech Company as a Public Actor

The United States depends on digital communications for much of our critical infrastructure, such as communications, delivery of electricity, or traffic control.[232] Digital communications are a matter of public importance but are largely controlled by private companies. Recognizing the networked nature of the country's cyber infrastructure and its attendant vulnerability, the Obama administration has sought to encourage the private sector to join a "Cybersecurity Framework."[233]

Increasing public-private partnerships may serve very real security needs that require collaboration and uniformity. These partnerships seek to stave off cybersecurity attacks, authorizing information sharing between private companies and the government and the employment of private subject-matter experts in the federal government.[234]

These partnerships, however, reduce the public-private divide, raising questions about the differences in objectives and responsibilities.[235] The collaboration makes it less likely a large corporation will view its security obligations as distinct from that of the government and will instead act like an agent of the government.[236] For example, larger tech companies appear less likely than smaller ones to challenge government requests for user information and related nondisclosure provisions.[237]

Collaboration in the form of a "Cybersecurity Framework" bears more than passing resemblance to the U.S. government's cooperation with AT&T in the 20th century to advance American science. As Tim Wu has observed, public-private partnership "goes a long way to explain how AT&T, as it matured, became in effect almost a branch of government, charged with top-secret work in the national interest."[238] If indeed many tech companies, acting

232. *See* Michael Daniel, *Improving the Security of the Nation's Critical Infrastructure*, WHITE HOUSE BLOG (Feb. 13, 2013, 6:39 PM), http://www.whitehouse.gov/blog/2013/02/13/improving-security-nation-s-critical-infrastructure.

233. Exec. Order No. 13,636, 3 C.F.R. 217, 219 (2014).

234. *See id.* at 218.

235. *See, e.g.*, PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 27, at 5–6.

236. Corporations do, however, retain interests distinct from the government, including corporate espionage, data breaches, and consumer confidence.

237. *Cf.* Miller, *supra* note 90 (observing that "[s]mall companies are more likely to take the government to court . . . because they have fewer government relationships and customers, and fewer disincentives to rock the boat"); Elena Schneider, *Technology Companies Are Pressing Congress to Bolster Privacy Protections*, N.Y. TIMES (May 26, 2014), http://www.nytimes.com/2014/05/27/us/technology-firms-press-congress-to-tighten-privacy-law.html (suggesting that after Snowden's revelations, smaller companies are more likely to comply with government requests because of their ignorance of legal requirements and litigation costs).

238. TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES 105 (2010).

in the national interest out of whatever motivation, be it security-minded patriotism or financial motivation, act like a government branch or agency, they may be less inclined to oppose government requests for user information.

Tech companies' roles as global players and commercial behemoths also explain why these companies may find common cause with the government. Information companies like AT&T and Verizon now rank among the world's 100 largest economic entities.[239] Amazon, Apple, and Yahoo!'s revenues similarly exceed that of many countries' gross domestic product.[240] Thus, their interests—financial, political, or security-related—will often coincide with that of other global powers, including the U.S. government.[241] Though their concerns may be legitimate, it raises the question of whether tech companies can effectively voice populist concerns of privacy over those of security and shared government interests.[242]

4. Tech Companies' Attitudes Toward Privacy

In the immediate wake of the Snowden leaks and news about the PRISM program,[243] Aaron Levie, CEO of Box.com, tweeted: "PRISM: Your Gmail, Google, Facebook, Skype data all in one place. The NSA just beat out like 30 startups to this idea."[244] Levie's tweet provides at least one explanation for tech companies' acquiescence to government requests for user information.

239. *See* TRACEY KEYS & THOMAS MALNIGHT, CORPORATE CLOUT: THE INFLUENCE OF THE WORLD'S LARGEST 100 ECONOMIC ENTITIES 9 (2012), *available at* http://www.globaltrends.com/images/stories/corporate%20clout%20the%20worlds%20100%20largest%20economic%20entities.pdf.

240. Vincent Trivett, *25 US Mega Corporations: Where They Rank If They Were Countries*, BUS. INSIDER (June 27, 2011, 11:27 AM), http://www.businessinsider.com/25-corporations-bigger-tan-countries-2011-6?op=1 (showing that "Amazon.com is bigger than Kenya . . . Apple is bigger than Ecuador [and] Yahoo is bigger than Mongolia").

241. *See, e.g.*, David Barboza, *Chinese Dissident, Jailed on Evidence Provided by Yahoo, Is Freed*, N.Y. TIMES (Aug. 31, 2012) http://www.nytimes.com/2012/09/01/world/asia/wang-xiaoning-chinese-dissident-in-yahoo-case-freed.html (describing a Chinese dissident's criminal conviction based on evidence Yahoo! provided to the Chinese government).

242. Most of the largest technological companies supported proposed legislation, the "Cyber Intelligence Sharing and Protection Act," notwithstanding the concerns of many privacy and civil liberties groups. *See* Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013); Gregory Ferenstein, *Hey Internet, Where's the Outrage?*, WASH. POST (Mar. 13, 2013, 2:27 PM), http://www.washingtonpost.com/blogs/innovations/post/hey-internet-wheres-the-outrage/2013/03/13/caf1f4b2-8c03-11e2-b63f-f53fb9f2fcb4_blog.html.

243. Gellman & Poitras, *supra* note 2.

244. Aaron Levie, TWITTER (June 6, 2013, 4:24 PM), https://twitter.com/levie/status/342783997232959488. A glib, if not hostile, attitude toward privacy has been a common perspective of Internet entrepreneurs. Scott McNealy, CEO of Sun Microsystems, said as early as 1999 that "[y]ou have zero privacy . . . . Get over it." Polly Sprenger, *Sun on Privacy: 'Get over It,'* WIRED (Jan. 26, 1999), http://www.wired.com/politics/law/news/1999/01/17538. Google CEO Eric Schmidt said, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." JEFF JARVIS, PUBLIC PARTS: HOW SHARING IN THE DIGITAL AGE IMPROVES THE WAY WE WORK AND LIVE 127 (2011) (internal quotation marks omitted).

The government's surveillance is not all that distinct from what many of the companies do, albeit with a different objective.[245] After all, "[t]he primary business model of the Internet is built on mass surveillance."[246] Thus, opposition to government surveillance might pose an almost existential crisis for many tech companies.

This is why tech companies have, at best, conflicted and often paradoxical positions regarding individual users' privacy. On the one hand, tech companies seek to acquire as much information as possible from users. On the other hand, to gain access to that information in the first place, many companies assure their users that their information will be private and secure.[247] And yet, they monetize the information by selling it to advertisers. As a result, tech companies have long preferred self-governance to regulation, arguing that restricting access to certain kinds of information could stunt online growth and innovation.[248] Though the early creators of the Internet and tech companies may have harbored anti-establishment, libertarian impulses, profit motives in an information-driven industry have reconfigured tech companies' relationship to users' privacy.[249]

5. Immunity

Tech companies also may decide to comply with government requests because of statutory immunity. FISA grants prospective immunity to communications providers as long as the Attorney General certifies the

245. Risen & Wingfield, *supra* note 213 (noting that both the NSA and Silicon Valley "hunt for ways to collect, analyze and exploit large pools of data about millions of Americans"); *see also* Richards, *supra* note 208, at 1938 (describing private companies' surveillance activities and stating that "[s]urveillance is not just for governments either").

246. Bruce Schneier, *The Public-Private Surveillance Partnership*, BLOOMBERG (July 31, 2013, 6:00 PM), http://www.bloombergview.com/articles/2013-07-31/the-public-private-surveillance-partnership.html. The public appears to recognize the twin-like "Big Brother" aspect to Internet surveillance, trusting a company like Google slightly less than the government. *See* Troy Mathew, *What's Worse Than Your Mom Seeing Your Web History? The NSA, Google*, SURVATA (Oct. 27, 2014), http://www.survata.com/blog/whats-worse-than-your-mom-seeing-your-web-history-the-nsa-google (reporting survey results finding that people would be slightly more concerned if Google had access to all their personal electrical data, rather than the government).

247. David Streitfeld & Quentin Hardy, *Data-Driven Tech Industry Is Shaken by Online Privacy Fears*, N.Y. TIMES (June 9, 2013), http://www.nytimes.com/2013/06/10/technology/data-driven-tech-industry-is-shaken-by-online-privacy-fears.html; *see also* Andrew Ross Sorkin, *Tech Companies Tread Lightly in Statements on U.S. Spying*, N.Y. TIMES DEALBOOK (June 10, 2013, 9:06 PM), http://dealbook.nytimes.com/2013/06/10/tech-companies-tread-lightly-in-statements-on-u-s-spying (stating how many companies deny that they give the U.S. government access to their data).

248. Claire Cain Miller, *Larry Page Defends Google's Privacy Policy*, N.Y. TIMES BITS (Oct. 17, 2012, 10:05 PM), http://bits.blogs.nytimes.com/2012/10/17/larry-page-defends-googles-privacy-policy; Claire Cain Miller, *Larry Page on Regulation, Maps and Google's Social Mission*, N.Y. TIMES BITS (Oct. 17, 2012, 9:58 PM), http://bits.blogs.nytimes.com/2012/10/17/larry-page-on-regulation-maps-and-googles-social-mission/; Streitfeld & Hardy, *supra* note 247.

249. *See* Miller, *supra* note 90; Streitfeld & Hardy, *supra* note 247.

companies properly acceded to government requests.[250] Coupled with the litigation costs, particularly legal challenges against the government over issues of law enforcement and security, these prospective statutory defenses from lawsuits may curb tech companies' instincts to challenge government requests.

But the precedent of retroactive immunity may also keep tech companies from challenging government requests. In the wake of litigation against telecommunications providers for cooperating with the Bush administration's warrantless Terrorist Surveillance Program, Congress passed the FISA Amendments Act ("FISAAA").[251] Section 802 of FISAAA authorized the dismissal of dozens of lawsuits against companies for actions taken pursuant to presidential directives.[252]

Congress elected to provide retroactive immunity precisely because of the incentives it would create.[253] Congress wanted to encourage private tech companies to cooperate with future government requests for user data.[254] As Senator Russ Feingold observed in opposing the immunity provisions, "[i]f we want [telecommunications providers] to obey the law in the future, doesn't it send a terrible message, doesn't it set a terrible precedent, to give them a 'get out of jail free' card for allegedly ignoring the law in the past?"[255] Thus, it seems clear Congress intended, and privacy advocates feared, that immunity provisions, both retroactive and prospective, would deter tech companies from fighting government requests for surveillance assistance.

250. *See* 18 U.S.C. §§ 2511(2)(a)(ii)(B), 2709(b) (2012); 50 U.S.C. §§ 1802(a)(4), 1805b(e) (repealed 2008), 1881a(h)(3), 1885a(a)(2), (3) (2012); *supra* Part III.C. (discussing the statutory enactment of the corporate avatar dynamic); *see also* ROCKEFELLER, *supra* note 210, at 12.

251. *In re* Nat'l Sec. Agency Telecomms. Records Litig., 671 F.3d 881, 891 (9th Cir. 2011).

252. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 201, 122 Stat. 2436, 2469 (codified as amended at 50 U.S.C. § 1885a(a)(4)(A)(i) (2012)) (immunizing companies for actions taken from September 11, 2001, through January 17, 2007).

253. S. REP. NO. 110-209, at 9, 11; *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 671 F.3d at 892–93.

254. *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 671 F.3d at 893 ("[I]f litigation were allowed to proceed against persons allegedly assisting in such activities, 'the private sector might be unwilling to cooperate with lawful Government requests in the future.'" (quoting S. REP. NO. 110-209, at 10)). Jon Michaels proposes a surveillance regime in which corporations would play a highly formalized role, complete with compliance and disclosure rules, as opposed to the "informal" role it took in the Terrorist Surveillance Program. Michaels, *supra* note 89, at 950–65. Private companies take on both Executive implementation functions and congressional oversight functions. *Id.* at 959–61. Among his many proposals, Michaels suggests immunity would induce corporations to participate in the program. *Id.* at 961–63.

255. 154 CONG. REC. S6381 (daily ed. July 8, 2008) (statement of Sen. Russ Feingold); *see also* Petition for a Writ of Certiorari at 40, Hepting v. AT&T Corp., 133 S. Ct. 421 (2012) (mem.) (No. 11-1200), 2012 WL 1097105, at *40 (arguing that the statute's grant of unfettered discretion to the Attorney General to certify that a provider merited immunity upset the separation of powers and empowered the Executive "to pressure telecommunications carriers to refrain from advocating the privacy rights of their customers").

The debate over tech company immunity also evidenced a strain of the corporate avatar dynamic. For example, the Senate Select Committee on Intelligence attributed its support of limits on the scope of immunity to providers' "essential role in ensuring that the Government complies with statutory requirements before collecting information that may impact the privacy interests of U.S. citizens."[256] And Senator Patrick Leahy insisted the statute "would subvert the gatekeeping role that FISA contemplates for the providers."[257] Whatever the merits of the argument that tech companies serve as a check on government abuse, statutory immunity reduces the likelihood that tech companies will resist government requests for assistance.[258]

B. COUNTERARGUMENT: THE MARKET AS A PRIVACY MOTIVATOR

Supporters of the corporate avatar dynamic might point to the marketplace's response to the Snowden leaks. The economic backlash has been significant.[259] Since news reports emerged of the tech companies' involvement in U.S. government surveillance, estimates of losses in the U.S. cloud computing industry range from $21.5 billion to $180 billion.[260] As a result, companies have sought to win back the public's trust and made efforts

256. S. REP. NO. 110-209, at 10.

257. PATRICK LEAHY, COMM. ON THE JUDICIARY, FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 AMENDMENTS ACT OF 2007, S. REP. NO. 110-258, at 20 (2008); *see also* Heidi Kitrosser, *It Came from Beneath the Twilight Zone: Wiretapping and Article II Imperialism*, 88 TEX. L. REV. 1401, 1430–31 (2010) (citing arguments concerning tech companies' government abuse-checking function).

258. It might be argued that tech companies act in the public interest, and therefore, their assistance with government surveillance justifies the same protections that state actors enjoy. *See supra* Part V.A.3 (discussing tech companies' government-like status); *see also* Filarsky v. Delia, 132 S. Ct. 1657, 1667–68 (2012) (holding that a private attorney hired to conduct an investigative interview for the government was entitled to claim qualified immunity under 42 U.S.C. § 1983); Michaels, *supra* note 89, at 962 n.268. Of course, if considered government actors, corporations' conduct would be subject to the limits of the Constitution. Jack Balkin has argued that it is precisely because the Constitution does not limit private behavior that the government involves the private sector in its surveillance. *See* Balkin, *supra* note 1, at 16–17.

259. *See, e.g.*, Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html (describing the reluctance of foreign nations to use American companies' tech services because of their susceptibility to, and compliance with, U.S. government surveillance).

260. SCHMIDT & COHEN, *supra* note 30, at 32–33 (arguing online information's vulnerability requires companies to ensure privacy and maintain user trust, or else the product will be abandoned); Nicole Perlroth & Vindu Goel, *Internet Firms Step Up Efforts to Stop Spying*, N.Y. TIMES (Dec. 5, 2013), http://www.nytimes.com/2013/12/05/technology/internet-firms-step-up-efforts-to-stop-spying.html (citing research showing cloud computing losses could reach $180 billion through 2016 as a result of NSA surveillance); Andrea Peterson, *NSA Snooping Could Cost U.S. Tech Companies $35 Billion over Three Years*, WASH. POST (Aug. 7, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/07/nsa-snooping-could-cost-u-s-tech-companies-35-billion-over-three-years (reporting that non-U.S. companies have cancelled contracts with U.S. cloud providers due to the NSA leaks, and that cloud providers may lose between $21.5 to $35 billion from 2013 through 2016).

to improve encryption,[261] publicize their efforts to withstand government surveillance,[262] limit their compliance with government data requests,[263] and tighten their privacy policies.[264] The Electronic Frontier Foundation credits these developments with corporations' improvements in resisting government requests for user data and general user advocacy.[265]

Moreover, globalization requires that companies serving customers in numerous countries meet those nations' laws that are often more protective of privacy.[266] Thus, corporations may need to improve their users' information security to placate European regulators and other nations.[267]

261. *See* Andrea Peterson, *Privacy Is Tech's Latest Marketing Strategy*, WASH. POST (Sept. 26, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/26/privacy-is-techs-latest-marketing-strategy/ (describing the marketing of products to appeal to privacy concerns); David E. Sanger & Brian X. Chen, *Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.*, N.Y. TIMES (Sept. 26, 2014), http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html (describing Apple's and Google's default encryption in the iPhone and Android, which make it impossible for the companies to comply with orders requiring the disclosure of users' content data); James B. Comey, Dir., Fed. Bureau of Investigation, Speech at the Brookings Institution: Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? (Oct. 16, 2014), *available at* http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (concluding that Apple's and Google' encryption of their devices "suggest that the post-Snowden pendulum has swung too far in one direction," while acknowledging that encryption will not affect data stored in the cloud or preclude access to metadata).

262. *See* David E. Sanger & Nicole Perlroth, *Internet Giants Erect Barriers to Spy Agencies*, N.Y. TIMES (June 6, 2014), http://www.nytimes.com/2014/06/07/technology/internet-giants-erect-barriers-to-spy-agencies.html (describing tech companies' litigation and ultimate deal with the government over disclosing the number of FISA requests).

263. *See, e.g.*, Schneider, *supra* note 237 (noting that Facebook, Twitter, and Google "will no longer hand over their customers' data without a search warrant").

264. *See, e.g.*, Vindu Goel, *Some Privacy, Please? Facebook, Under Pressure, Gets the Message*, N.Y. TIMES (May 22, 2014), http://www.nytimes.com/2014/05/23/technology/facebook-offers-privacy-checkup-to-all-1-28-billion-users.html (describing Facebook's changes to privacy policies, including a default privacy setting and an individual privacy checkup for users).

265. *See* NATE CARDOZO ET AL, ELEC. FRONTIER FOUND., WHO HAS YOUR BACK? PROTECTING YOUR DATA FROM GOVERNMENT REQUESTS: THE ELECTRONIC FRONTIER FOUNDATION'S FOURTH ANNUAL REPORT ON ONLINE SERVICE PROVIDERS' PRIVACY AND TRANSPARENCY PRACTICES REGARDING GOVERNMENT ACCESS TO USER DATA 7 (2014), *available at* https://www.eff.org/files/2014/05/15/who-has-your-back-2014-govt-data-requests.pdf (attributing the "major improvements in industry standards for informing users about government data requests, publishing transparency reports, and fighting for the user in Congress" to revelations about "a close relationship between tech companies and [the government]").

266. *See, e.g.*, Danny Hakim, *Right to Be Forgotten? Not That Easy*, N.Y. TIMES (May 29, 2014), http://www.nytimes.com/2014/05/30/business/international/on-the-internet-the-right-to-forget-vs-the-right-to-know.html (describing Google's efforts to comply with the Court of European Union's decision that the "right to be forgotten" outlined in the European Union's 1995 Privacy Directive required Google to grant individuals' requests to remove inaccurate and irrelevant personal information); *see also* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 EUR-Lex 62012CJ0131 (May 13, 2014).

267. Michael J. Geary & Kevin A. Lees, *NSA Scandal Will Follow Obama to Europe*, NAT'L INT. (June 14, 2013), http://nationalinterest.org/commentary/nsa-scandal-follows-obama-europe-8602 (noting that service providers may be subjected to European lawsuits and regulation);

Government officials in India are prohibited from using email connected to servers in the United States.[268] And Germany and Brazil have warned that they may only permit data to go through local providers.[269]

Since the Snowden revelations, tech companies have engaged in highly publicized litigation against the government over surveillance.[270] For example, Facebook has challenged sealed search warrants for 381 user accounts, including their photos, likes, messages, and comments.[271] Facebook also attacked the warrants' nondisclosure provisions, contending that "[t]he people whose accounts are the targets of the searches deserve the opportunity to contest the seizure of their information in advance."[272] The focus on notice to the user reflected the company's appreciation of its own limitations in approximating individual users' reactions to the government's acquiring their personal information.

Microsoft has similarly publicized its efforts to quash a warrant for email contents, which Microsoft argues are stored in a Dublin, Ireland, data center and are therefore outside the federal courts' jurisdiction.[273] AT&T, Apple, Cisco, and Verizon filed amicus curiae briefs in support of Microsoft.[274]

Sanger & Perlroth, *supra* note 262 (noting a decline in hardware companies' business in Asia, Brazil, and Europe since the Snowden leaks); *see also* Mark Scott, *Where Tech Giants Protect Privacy*, N.Y. TIMES (Dec. 13, 2014), http://www.nytimes.com/2014/12/14/sunday-review/where-tech-giants-protect-privacy.html (attributing Silicon Valley companies' privacy improvements to European regulations).

268. *See* Perlroth & Goel, *supra* note 260.

269. *See id.*; Sanger & Perlroth, *supra* note 262.

270. The most immediate litigious response by tech companies was the tech companies' lawsuit to permit more detailed reporting of FISA and NSL requests by the government. *See, e.g.*, Motion for Declaratory Judgment of Google Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders, *supra* note 169, at 4. Tech companies have also sought legislative reform of NSA surveillance. *See, e.g.*, Chris Strohm, *Facebook, Apple Make Year-End Lobbying Push to Curb NSA Spying*, BLOOMBERG (Nov. 14, 2014, 2:45 PM), http://www.bloomberg.com/news/2014-11-14/companies-call-on-senate-to-pass-bill-curbing-nsa-powers.html.

271. *See* Memorandum of Law in Support of Facebook, Inc.'s Motion to Quash Bulk Search Warrants and Strike Nondisclosure Provisions, *In re* 381 Search Warrants Directed to Facebook, Inc. and Dated July 23, 2013, No. 30207-13 (N.Y. Sup. Ct. Aug. 20, 2013); Vindu Goel & James C. McKinley Jr., *Forced to Hand Over Data, Facebook Files Appeal*, N.Y. TIMES (June 26, 2014), http://www.nytimes.com/2014/06/27/technology/facebook-battles-manhattan-da-over-warrants-for-user-data.html; James C. McKinley Jr., *Court Weighs Facebook's Right to Challenge Search Warrants on Users' Behalf*, N.Y. TIMES (Dec. 11, 2014), http://www.nytimes.com/2014/12/12/nyregion/court-weighs-facebooks-right-to-challenge-search-warrants-on-users-behalf.html.

272. Memorandum of Law in Support of Facebook, Inc.'s Motion to Quash Bulk Search Warrants and Strike Nondisclosure Provisions, *supra* note 271, at 7.

273. *See In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 467 (S.D.N.Y. 2014); Joseph Ax, *Microsoft Ordered by U.S. Judge to Submit Customer's Emails from Abroad*, REUTERS (July 31, 2014, 1:33 PM), http://www.reuters.com/article/2014/07/31/us-usa-tech-warrants-idUSKBN0G024I20140731; Brad Smith, Op-Ed., *We're Fighting the Feds over Your Email,* WALL ST. J. (July 29, 2014, 7:35 PM), http://www.wsj.com/articles/brad-smith-were-fighting-the-feds-over-your-email-1406674616.

274. Ax, *supra* note 273.

Though much of the rhetoric focuses on privacy, the tech companies' aggressive litigation stance is no doubt stimulated in part by customers' perceptions that their data are vulnerable to U.S. surveillance, regardless of where the data are stored and the fact that they may opt to use different services.[275]

It may be too early to tell whether the market will compel tech companies to make long-term changes to their privacy policies and compliance with government requests for user data. First, notwithstanding many of the protests over surveillance and inadequate privacy protections, many foreign users remain "hooked" or prefer to use U.S. companies' services.[276] Second, legal requirements, in particular nondisclosure, may prevent companies from strengthening privacy and other user protections from government data requests.[277] Third, companies may choose not to alter their current relationship with the government given their many economic and entrenched mutually beneficial connections.[278] Fourth, companies may not want to appear unpatriotic by increasing user privacy protection at a perceived expense of national security.[279] Finally, many companies may announce changes to their privacy policies in the Snowden aftermath, without making any long-term alterations. Privacy policies are notoriously malleable; companies unilaterally change the terms frequently.[280]

But let us accept that external forces presage a change in tech companies' compliance with government requests for user data and surveillance assistance. Even a radical transformation of the intelligence-industrial complex cannot save the corporate avatar dynamic. As the next Part argues, inserting the private tech company as the voice and conscience of the people wreaks havoc with the history and purposes of the Fourth Amendment.

275. *See, e.g.*, Memorandum of Law in Support of Verizon Commc'ns' Motion to Participate as Amicus Curiae and Microsoft's Motion to Vacate Search Warrant at 1–2, *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 466 (S.D.N.Y. June 10, 2014), ECF No. 29 (noting warrants' potential "enormous detrimental impact on the international business of American companies, on international relations, and on privacy."); Ax, *supra* note 273.

276. *See* Mark Scott, *Principles Are No Match for Europe's Love of U.S. Web Titans*, N.Y. TIMES (July 6, 2014), http://www.nytimes.com/2014/07/07/technology/principles-are-no-match-for-europes-love-of-us-tech-titans-like-amazon-and-facebook.html (noting that U.S. tech companies constitute "seven of the [ten] most visited websites in Europe").

277. *See supra* Part IV.B; *see also* Michaels, *supra* note 89, at 940–41.

278. *See supra* Part V.A.1; *see also* Michaels, *supra* note 89, at 940–42.

279. Michaels, *supra* note 89, at 941–42.

280. *Id.* at 941. In addition, purported improvements to privacy policies may easily sway people without resulting in much change at all. *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1066 n.222 (2012) (noting that many people assume the fact of a privacy policy indicates that a company will not share their data with third parties).

C. THE NORMATIVE WEAKNESSES OF THE CORPORATE AVATAR DYNAMIC

1. The Fourth Amendment as a Check on Government

In addition to protecting privacy interests, the Fourth Amendment affords "a means of preserving the people's authority over government—the people's sovereign right to determine how and when government may intrude into the lives and influence the behavior of its citizens."[281] Canvassing pre-constitutional history, Raymond Ku argues that the Fourth Amendment is best viewed as "an outgrowth and complement to the limitations placed upon executive power through the Constitution's separation of powers."[282]

Akhil Reed Amar interprets the Fourth Amendment's phrase "the people" as demonstrating a "concern with the agency problem of protecting the people generally from self-interested government policy."[283] The Bill of Rights limits government officials (the people's "agents") from governing against the interests of the people (the "principals").[284] Under this holistic understanding of the Fourth Amendment, the Framers intended for "the people"—in connection with the exercise of the Seventh Amendment right to a jury—to determine the reasonableness of searches in civil lawsuits for trespass against government officials.[285]

The Framers viewed judicially-issued warrants, on the other hand, with skepticism. Warrants were unlikely to deter "government overreaching" because they issued from a solitary government official whose decision was made in secret, without notice or an adversarial proceeding.[286] The Framers thus envisioned a "populist Fourth Amendment."[287] This populist perspective—which stresses accountability and balancing of government powers—makes vesting the power to challenge Fourth Amendment violations in tech companies, instead of "the people," constitutionally incoherent.

2. English History of Corporate Searches and Seizures

Scholars and courts have frequently looked to English history and case law on the legislation of broad and general search-and-seizure powers, particularly general warrants, in explicating the Fourth Amendment.[288] But

281. Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1326 (2002).

282. *Id.* at 1332–33; *see also id.* at 1343 (identifying as important the principle that the Fourth Amendment "is intended to limit executive power and discretion").

283. AKHIL REED AMAR, THE BILL OF RIGHTS: CREATION AND RECONSTRUCTION 68 (1998).

284. *Id.* at xiii.

285. *Id.* at 68, 70–75; *see also* AKHIL REED AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE: FIRST PRINCIPLES 10–17 (1997); Ku, *supra* note 281, at 1338–39.

286. AMAR, *supra* note 283, at 69; *see also id.* at 70 (observing that government could also "forum shop," seeking out the sympathetic magistrate judge for a warrant).

287. *Id.* at 73.

288. *See, e.g.*, Boyd v. United States, 116 U.S. 616, 626–27 (1886) ("[I]t may be confidently asserted that [*Entick*'s] propositions were in the minds of those who framed the Fourth

the role that private corporations played in these searches has received less attention. Though the Fourth Amendment does not refer to searches by private corporations on behalf of the government, the Framers were doubtless aware that the expansive search-and-seizures powers originated with the authorization of the Stationers' Company to conduct searches to support both the government licensing system that imposed censorship and prior restraints and the company's monopoly on the printing industry.[289]

In 1566, the King's Council decreed that officers from the Stationers' Company had the authority to search all locations, open all packages of papers and books, seize books violating any statutes or proclamations, and receive half of the proceeds from fines levied by the king.[290] Company officials were particularly inclined to search in their own interest.[291] Guild members that were granted exclusive printing licenses often received the related authority to enter and search "all suspected places" to maintain their monopoly.[292] From 1623 to 1629, Stationers exercised their search powers and seized more than 20,000 texts, including Bibles, from Cambridge University.[293]

The Stationers' Company's expansive search-and-seizure powers played a vital part in censoring and suppressing sedition and dissent, reflecting its role "as an executive tool of the Government."[294] During the 17th century, the

Amendment to the Constitution, and were considered as sufficiently explanatory of what was meant by unreasonable searches and seizures."); Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.) [812] (appeal taken from C.B.) (holding in a trespass action against government officials and messengers that general warrants and the resulting search of homes and seizure of materials critical of the King were "contrary to the genius of the law of England"); Wilkes v. Wood, (1763) 98 Eng. 489 (K.B.) (appeal taken from C.B.); NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 22–50 (1937) (describing early English history of search and seizure).

289. Marcus v. Search Warrants of Prop. at 104 E. Tenth St., Kansas City, Mo., 367 U.S. 717, 724–25 (1961) (describing Stationers' Company's search-and-seizure powers in furtherance of the Tudor licensing system); *id.* at 729 ("This history was, of course, part of the intellectual matrix within which our own constitutional fabric was shaped. The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."); WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 602–1791, at 58–60 (2009); FREDERICK SEATON SIEBERT, FREEDOM OF THE PRESS IN ENGLAND 1476–1776: THE RISE AND DECLINE OF GOVERNMENT CONTROL 374–76 (Univ. of Ill. Press, Urbana, 1965) (1952); Thomas B. Nachbar, *Intellectual Property and Constitutional Norms*, 104 COLUM. L. REV. 272, 320 (2004).

290. JACOB W. LANDYNSKI, SEARCH AND SEIZURE AND THE SUPREME COURT: A STUDY IN CONSTITUTIONAL INTERPRETATION 22–23 (1966) (describing the company's regulations requiring that printing houses be subject to a weekly search by printers and that printers be made easily accessible for searches); LASSON, *supra* note 288, at 24–25; *see also Marcus*, 367 U.S. at 724–29; Wheaton v. Peters, 33 U.S. 591, 670 (1834).

291. CUDDIHY, *supra* note 289, at 92–93.

292. *Id.* at 93 (internal quotation marks omitted).

293. *Id.*

294. CYPRIAN BLAGDEN, THE STATIONERS' COMPANY: A HISTORY, 1403–1959, at 70 (1960); *see* CUDDIHY, *supra* note 289, at 59; LANDYNSKI, *supra* note 290, at 20–23; *see also Marcus*, 367 U.S. at

company's search powers broadened beyond searches of printing houses to include any suspected locations, without geographic limitation.[295] The English government manipulated the Stationers' Company's monopolistic aims to serve its own ends. This exploitation crystallizes the incongruity of appointing powerful corporations to guard against government surveillance today.

3. Constitution-Era Distrust of Corporations

Colonial history also suggests that the Framers viewed private corporations with "distrust or disfavor."[296] American Revolution history reflects the colonists' frustration at the admixture of government overreaching and corporate dominance.[297] Indeed, the Boston Tea Party was the apotheosis of early American resentment of unfettered government-corporate monopolistic power—a rejection of both the East India Company's government-granted monopoly on American tea and onerous taxes.[298]

At the time of the founding, many called for a provision, explicitly prohibiting corporate monopolies.[299] Thomas Jefferson argued for a "restriction against monopolies" within the Bill of Rights.[300] For Jefferson, guarding against the encroachment on liberty by the Legislative and Executive branches entailed restricting corporate monopolies.

---

724 (describing Stationers' Company's incorporation and searching authority as "a principal instrument for the enforcement of the Tudor licensing system").

295. *Marcus*, 367 U.S. at 725–27; CUDDIHY, *supra* note 289, at 59, 173–74, 304–05, 427.

296. 1 WILLIAM MEADE FLETCHER, FLETCHER CYCLOPEDIA OF THE LAW OF CORPORATIONS § 2, at 7 (rev. vol. 2006); *see also* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 426–27 (2010) (Stevens, J., concurring in part and dissenting in part) (describing early American criticism of corporations).

297. Steven G. Calabresi & Larissa C. Leibowitz, *Monopolies and the Constitution: A History of Crony Capitalism*, 36 HARV. J.L. & PUB. POL'Y 983, 1008 (2013) (describing how "England's monopolistic trade laws led to protest by the colonists and eventually the American Revolution"); Jonas V. Anderson, Note, *Regulating Corporations the American Way: Why Exhaustive Rules and Just Deserts Are the Mainstay of U.S. Corporate Governance*, 57 DUKE L.J. 1081, 1100–01 (2008).

298. NICK ROBINS, THE CORPORATION THAT CHANGED THE WORLD: HOW THE EAST INDIA COMPANY SHAPED THE MODERN MULTINATIONAL 110–15 (2d ed. 2012); HARLOW GILES UNGER, AMERICAN TEMPEST: HOW THE BOSTON TEA PARTY SPARKED A REVOLUTION 159–60 (2011); Calabresi & Leibowitz, *supra* note 297, at 1008 (describing the Boston Tea Party as "an act against the British government *and the East India Company*, which had a monopoly over tea importations to the colonies").

299. Calabresi & Leibowitz, *supra* note 297, at 1009–15 (describing the opposition to monopolies at the time of the nation's founding); *id.* at 1013 (noting that six states sought a ban on monopolies in the U.S. Constitution). *But see* Nachbar, *supra* note 289, at 344 ("[T]here is no indication that the concern over the possibility of federal monopolies was widespread.").

300. Letter from Thomas Jefferson to James Madison (Dec. 20, 1787), *in* 5 THE WORKS OF THOMAS JEFFERSON 368, 371 (Paul Leicester Ford ed., 1904); *see also* THOM HARTMANN, UNEQUAL PROTECTION: HOW CORPORATIONS BECAME "PEOPLE"—AND YOU CAN FIGHT BACK 89–91 (2d ed. 2010) (describing Jefferson's continued calls for freedom from monopolies); Calabresi & Leibowitz, *supra* note 297, at 1009–12. *But see* Nachbar, *supra* note 289, at 341 (describing Jefferson's views as "extremist[ ]" and "hardly representative of the views of the Framers").

Although James Madison did not support an anti-monopoly amendment to the Constitution, he strongly disfavored monopolies.[301] In describing his conception of republican government, Madison wrote that it must:

> [B]e derived from the great body of the society, not from an inconsiderable proportion, or a favored class of it; otherwise a handful of tyrannical nobles, exercising their oppressions by a delegation of their powers, might aspire to the rank of republicans, and claim for their government the honorable title of republic.[302]

But inserting corporations as the peoples' avatars hardly realizes the Framers' populist objectives.

Although today there is far greater concern over private monopolies than government-sponsored ones, the general worry is the same: corruption and abuses that benefit a private few over the general public.[303] Given the Framers' awareness of the Stationers' Company's history and antipathy toward corporations, it is hard to conceive of their assent to a Fourth Amendment that relies on corporate challenges on behalf of the people.[304]

4. Fourth Amendment Minority Viewpoint Protection

Another purpose of the Fourth Amendment is "to afford shelter to political, religious, and ideological minorities."[305] Leaving it to tech companies' discretion to oppose government requests for information pertaining to minority interests hardly supports that purpose. While tech companies, particularly social media, may speak "in the language of freedom and liberation," Evgeny Morozov argues that the idealistic rhetoric "allows vested interests to disguise what essentially amounts to advertising for their commercial products."[306] At bottom, a company is understandably motivated

301. Calabresi & Leibowitz, *supra* note 297, at 1014–16.

302. THE FEDERALIST NO. 39, at 193 (James Madison) (Ian Shapiro ed., 2009).

303. *See* Calabresi & Leibowitz, *supra* note 297, at 1056–57 (describing the evolution of concern from government grants of exclusive privileges to one of "crony capitalism").

304. Thomas Nachbar cautions against inferring a constitutional norm from some of the Framers' anti-monopoly statements. Nachbar, *supra* note 289, at 344–45 (arguing that there is a lack of "'demonstrable consensus' that an originalist would expect to see before inferring an effect on the meaning of the Constitution" (quoting Edwin Meese, III, U.S. Attorney Gen., Construing the Constitution: Address Before the D.C. Chapter of the Federalist Society Lawyers Division (Nov. 15, 1985), *in* 19 U.C. DAVIS L. REV. 22, 26 (1985))). Rather than proposing a narrow anti-monopoly constitutional norm, I adopt Amar's conception of a "populist Fourth Amendment," which integrates the historical background of skepticism of corporate monopolies and their role in searches and seizures. AMAR, *supra* note 283, at 73; *see also* Marcus v. Search Warrants of Prop. at 104 E. Tenth St., Kansas City, Mo., 367 U.S. 717, 729 (1961).

305. STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 141 (2012); *see also* AMAR, *supra* note 283, at 67–68.

306. EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM 304 (2011).

by financial profit. The messianic zeal of Internet futurists and Google's "don't be evil"[307] incantation should not dispel that notion.

The financial motive means a tech company focuses on giving the majority of the public what it wants. As Facebook CEO Mark Zuckerberg puts it, "We view it as our role in the system to constantly be innovating and be updating what our system is to reflect what the current social norms are."[308] Mirroring the norms on privacy and tolerance of government or corporate intrusion and surveillance may be good business, but it is not the proper basis for protecting constitutional rights. As corporate entities that are accountable to their shareholders and that seek to serve as much of the majority and the mainstream as possible, tech companies cannot fulfill the Fourth Amendment's aims as avatars for minority expression and information.

5. The Corporate Fourth Amendment Right

Over the past two centuries, corporations have taken on the vestiges of personhood, including individual rights provided in the Constitution.[309] But unlike the expansion of First Amendment rights, a corporation's Fourth Amendment rights remain limited.[310] The Supreme Court "has recognized that a business, by its special nature and voluntary existence, may open itself to intrusions that would not be permissible in a purely private context."[311] Hence, commercial property owners do not enjoy the same expectation of

307. Samuel Gibbs, *Google Has "Outgrown" Its 14-Year Old Mission Statement, Says Larry Page*, GUARDIAN (Nov. 3, 2014, 9:26 AM), http://www.theguardian.com/technology/2014/nov/03/larry-page-google-dont-be-evil-sergey-brin.

308. Marshall Kirkpatrick, *Facebook's Zuckerberg Says the Age of Privacy Is Over*, READWRITE (Jan. 9, 2010), http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov (quoting Mark Zuckerberg) (internal quotation marks omitted); *see also* Jeffrey Rosen, *The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google*, 80 FORDHAM L. REV. 1525, 1535 n.48 (2012).

309. *See* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 365 (2010) (holding that a "corporate identity" may not restrict its First Amendment Right to free speech). *See generally* Carl J. Mayer, *Personalizing the Impersonal: Corporations and the Bill of Rights*, 41 HASTINGS L.J. 577 (1990) (describing the evolution of the rights corporations enjoy).

310. *See* Christopher Slobogin, Citizens United *&* *Corporate & Human Crime*, 14 GREEN BAG 2D 77, 83 (2010) ("Right now, corporations have virtually no Fourth Amendment rights where it really counts."); William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1037 (1995) ("Fourth Amendment law protects corporations, but only nominally."). *But see* Burwell v. Hobby Lobby Stores, Inc., 134 S. Ct. 2751, 2768 (2014) ("[E]xtending Fourth Amendment protection to corporations protects the privacy interests of employees and others associated with the company."); Hale v. Henkel, 201 U.S. 43, 76 (1906) ("[W]e do not wish to be understood as holding that a corporation is not entitled to immunity, under the Fourth Amendment, against *unreasonable* searches and seizures."); Palmat Int'l, Inc. v. Holder, No. 12-20229-CIV, 2013 WL 594695, at *4 n.5 (S.D. Fla. Feb. 14, 2013) ("It is unclear whether the right to informational privacy extends to corporations.").

311. G.M. Leasing Corp. v. United States, 429 U.S. 338, 353 (1977).

privacy as do individual homeowners.[312] And subpoenas for corporate records often do not offend the Fourth Amendment.[313]

In addressing the reasonableness of corporate subpoenas, the Supreme Court expounded on the reasons for a corporation's adumbrated right to privacy:

> [C]orporations can claim no equality with individuals in the enjoyment of a right to privacy. They are endowed with public attributes. They have a collective impact upon society, from which they derive the privilege of acting as artificial entities. The Federal Government allows them the privilege of engaging in interstate commerce. Favors from government often carry with them an enhanced measure of regulation.[314]

Justice O'Connor more recently explained that because it "is an artificial being," a corporation "is not entitled to purely personal guarantees whose historic function . . . has been limited to the protection of individuals."[315] As a result, according to Justice O'Connor, a corporation does not have a right to privacy.[316] As the Court has repeatedly made clear, corporations bear little resemblance to individuals and their relationship to the government is also decidedly different from that of the people to the government. Rather, corporations bear some similarity to the government's functions and also owe their very existence to the government. Such a description of the corporation is hard to reconcile with the notion of corporations as the people's avatars.[317]

6. The Dangerous Power of the Private Few

When the Fourth Amendment is viewed as "a way to constrain the power of the state to regulate," leaving enforcement of the right against

312. Dow Chem. Co. v. United States, 476 U.S. 227, 237–38 (1986) (citing Donovan v. Dewey, 452 U.S. 594, 598–99 (1981)).

313. United States v. Morton Salt Co., 338 U.S. 632, 651–53 (1950); *see also* Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 66 (1974) (noting that the government's "requirements for the reporting of domestic financial transactions abridge no Fourth Amendment right of the banks themselves").

314. *Morton Salt Co.*, 338 U.S. at 652 (citations omitted); *see also Hale*, 201 U.S. at 75 (explaining that as a creature of the state a corporation may be more subject to searches).

315. Browning-Ferris Indus. of Vt., Inc. v. Kelco Disposal, Inc., 492 U.S. 257, 284 (1989) (O'Connor, J., concurring in part, dissenting in part) (internal quotation marks omitted); *see also* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 466 (2010) (Stevens, J., concurring in part, dissenting in part) ("[C]orporations have no consciences, no beliefs, no feelings, no thoughts, no desires. . . . [T]hey are not themselves members of 'We the People' by whom and for whom our Constitution was established."). *But see Burwell*, 134 S. Ct. at 2768 ("A corporation is simply a form of organization used by human beings to achieve desired ends.").

316. *Browning-Ferris Indus. of Vt., Inc.*, 492 U.S. at 284.

317. If, along the same rationale of *Citizens United*, Christopher Slobogin conjectures, the Supreme Court accorded greater Fourth Amendment protections to corporate records, then it might be harder for the government to obtain a corporation's customer's personal data. Slobogin, *supra* note 310, at 85. But Slobogin doubts that corporate agitation will ultimately precipitate change in the law. *Id.* at 85–86.

unreasonable searches and seizures to a handful of companies is deeply troubling.[318] The small number of tech companies that dominate telecommunications and the Internet make them more susceptible to interests that do not favor privacy protection or government oversight.[319]

Tim Wu has made a similar observation about free speech, contending that the "'speech industry'—as we might term any information industry—once centralized, becomes an easy target for external independent actors with strong reasons of their own for limiting speech."[320] As Wu argues, "[I]n the United States, it is industrial structure that determines the limits of free speech."[321]

Industrial structure may well dictate the contours of privacy. At some level, it is simple mathematics. Because of the immense power that just a few telecommunications carriers and Internet companies hold over our data, the government does not need many entities to undertake large-scale surveillance.[322] As a result, there is less opportunity for challenges by entities. Moreover, the powerful positions held by a Google or Amazon owe much to relationships with the government that they may not want to risk over requests for consumer data.[323] In addition, just a few powerful companies may defeat users' expectations of privacy from government intrusion by drafting contracts that afford the companies broad rights of access, collection, and analysis to users' contents and data.[324]

This dynamic is in and of itself a threat to democratic accountability and the Fourth Amendment. The widespread use of information technologies that are owned by a few companies reduces the checks and balances that

318. LESSIG, *supra* note 7, at 213; *see also* Stuntz, *supra* note 310, at 1026.

319. *See* Farhad Manjoo, *The Great Tech War of 2012: Apple, Facebook, Google, and Amazon Battle for the Future of the Innovation Economy*, FAST COMPANY (Oct. 19, 2011, 5:00 AM), http://www.fastcompany.com/1784824/great-tech-war-2012 (describing Amazon, Apple, Facebook, and Google as the most important companies determining the economy's agenda).

320. WU, *supra* note 238, at 122–23; *see also id.* at 273 (arguing that Google and Apple "are determining how Americans and the rest of the world will share information").

321. *Id.* at 121; *see also* Rosen, *supra* note 308, at 1536–37 (observing that tech companies may remove material that offends some portion of the community without violating the First Amendment); David Goldman, *Google: The Reluctant Censor of the Internet*, CNN MONEY (Jan. 4, 2015, 9:24 AM), http://money.cnn.com/2015/01/04/technology/google-censorship/index.html (describing Google's removal of content and links at the request of countries, including the United States).

322. JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 117–18 (2008).

323. *See supra* Part V.A.1. The relative low cost and secrecy of technology-aided surveillance for the government also raise concerns over checks and balances. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring); *id.* at 963–64 (Alito, J., concurring); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 674 (2011).

324. United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010) ("[I]f the ISP expresses an intention to 'audit, inspect, and monitor' its subscriber's emails, that might be enough to render an expectation of privacy unreasonable." (citations omitted)).

government had to overcome in the past to conduct surveillance.[325] Today, the co-option (or cooperation) of one entity can effect extensive surveillance.[326] Similarly, the fewer companies that hold sway over the Internet and telecommunications, the easier it is for the government to leverage the companies' commercial interests and induce them to make changes to the technologies that will facilitate surveillance.[327]

VI. SOLUTIONS TO THE CORPORATE AVATAR DYNAMIC FALLACY

Accepting that corporate avatars will not advocate for individuals' privacy rights and that the corporate avatar dynamic undermines separation of powers, what is the solution? How can individual users obtain their own agency? The clearest answer is to provide users with notice of the government's request for their information, be it content or non-content data.

The right to notice, however, must follow from a change in understanding of individuals' relationship to their data and how we define privacy. First, the third-party doctrine should be limited by affording Fourth Amendment protection to some non-content data and eliminating the conceit that disclosure of personal data to tech companies is voluntary.

Second, individual users, not simply the companies that acquire and analyze their data, should retain a proprietary right in their data. Based on the property interest in data, individuals should receive notice before the government acquires their data from third-party corporations.

Third, the proprietary and resulting privacy interests should be communicated as much as possible and at the earliest stage by individuals' machines to government and corporations' machines. Securing individual privacy and limits on government overreach in the big data era require changes in the way people, companies, and government interact through technological devices. Because of the countless ways in which we share data through tech companies (and the government) it is nearly impossible to know how and when data are used and when notice might be warranted. By operationalizing these interests through automation at the front end, corporations and the government will know what information may be obtained and what information may require the intervention of a court. Finally, as an adjunct to the automated process, greater transparency is necessary to better understand how both companies and the government use individuals' data.

325. ZITTRAIN, *supra* note 322, at 117–18.

326. *Id.*

327. LESSIG, *supra* note 7, at 61–62; *see also id.* at 80 ("Commerce has a purpose, and government can exploit that to its own end. It will, increasingly, and more frequently, and when it does, the character of the Net will change.").

A. NOTICE

Providing notice to the user when the government requests data is necessary to realize the populist and government-limiting purposes of the Fourth Amendment. Even at the third-party doctrine's origins, Justice William Brennan decried the lack of notice as "a fatal constitutional defect."[328]

Notice affords individuals the opportunity to challenge requests themselves or in conjunction with the company. Usually, the user will have a greater stake in the personal information at issue and thus, be more knowledgeable and more incentivized to challenge the government.[329]

When the government seeks records from a third-party company, there is usually no concern that evidence will be destroyed.[330] Records for which businesses often hold copies or can easily duplicate the data should not therefore present a problem.

There are, however, instances in which providing notice could harm law enforcement and security interests.[331] But, as Chief Justice Roberts has acknowledged, "[p]rivacy comes at a cost."[332] Where security and law enforcement concerns necessitate secrecy, the government should be required to obtain a warrant. In other exigent circumstances, the law allows for warrantless searches and other mechanisms for preserving data while waiting for a warrant.[333]

B. LIMITING THE THIRD-PARTY DOCTRINE

Justice Sotomayor's exhortation in *Jones* to "reconsider" [334] the third-party doctrine is particularly compelling in the big data era, in which (1) big data is employed to discover intimate and personal habits and beliefs based on non-content information; and (2) disclosure of personal information to third parties is the price—not the voluntary choice—of participation in society. Applying *Smith* to its logical conclusion today would make the third-party doctrine not the exception but the rule, and eviscerate Fourth Amendment application to countless data bearing on personal and intimate matters.

328. United States v. Miller, 425 U.S. 435, 448 n.2 (1976) (Brennan, J., dissenting).

329. *See* State v. Reid, 945 A.2d 26, 35 (N.J. 2008); CARDOZO ET AL., *supra* note 142, at 10.

330. *See* SCHULHOFER, *supra* note 305, at 134.

331. *See, e.g.*, *Reid*, 945 A.2d at 36. The New Jersey Supreme Court held that Internet users have a reasonable expectation of privacy in the subscriber information they give to the ISP, but did not require that notice be provided to users due to concerns that evidence might be destroyed. *Id.* at 28, 36. The court's reasoning suggests that in instances where the third-party company has copies or back-ups of the data, notice should be required. *See id.* at 36.

332. Riley v. California, 134 S. Ct. 2473, 2493 (2014).

333. *See id.* at 2483–84; SCHULHOFER, *supra* note 305, at 134.

334. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

1. Non-Content Data Exception

The third-party doctrine should not apply to a person's "non-content" data. The data at issue in *Smith* do not compare to the "quantity and variety" of big data, or to the "analytics" that may be applied to the data.[335] The *Smith* Court could not have contemplated "that the traces of digital data left today as a matter of routine can be reassembled to reveal intimate personal details."[336]

At the heart of the content/non-content distinction is an archaic conceit that content information encompasses information more deserving of privacy. But to the extent big data permits an understanding of a person's individual behavior over lengthy periods of time, it is just as intrusive as accessing a person's communication contents.[337] However the information may be defined, the Internet will contain even more personal information in the near future, monitoring all our activities, from the beat of our hearts to videos we watch.[338]

Cases that have held that metadata do not merit Fourth Amendment protection have focused on that information's purported imprecision; the courts predicate their holdings on the idea that the information only serves as fodder for "educated guesses" and speculation about the contents of communications.[339] But the ever-increasing use of communication devices and capabilities of data analytics render the content/non-content distinction obsolete in terms of guarding protection.

As Judge Garaufis recognized, "there is no meaningful Fourth Amendment distinction between content and other forms of information, the disclosure of which to the Government would be equally intrusive and reveal information society values as private."[340] Judge Leon similarly emphasized that the amount and quality of big data analytics means "[r]ecords that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person's

335. *See* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 27, at 19.

336. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 49 (2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf; *see also id.* at 34 (noting that "with the advent of big data," metadata, such as originating and terminating phone numbers, may be as revealing as the phone conversation and merit the same privacy protections).

337. *See Riley*, 134 S. Ct. at 2490 (observing that website visits and search terms can reveal private interests and that CSLI can reveal a person's whereabouts).

338. *See* Quentin Hardy, *They Have Seen the Future of the Internet, and It Is Dark*, N.Y. TIMES BITS (July 5, 2014, 7:00 AM), http://bits.blogs.nytimes.com/2014/07/05/they-have-seen-the-future-of-the-Internet-and-it-is-dark/.

339. United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007).

340. *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 125 (E.D.N.Y. 2011) (citing Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979)).

life."[341] Thus, the government's acquiring and analyzing metadata and other "non-content" may be as great a privacy intrusion as any surveillance of "content" data.[342] The advances of big data therefore require an exception to the third-party doctrine for non-content data as well.

2. Involuntary Provision of the Personal Data Exception

The third-party doctrine in the big data era is also hard to justify based on its original voluntariness rationale. In an increasingly connected world, choosing not to provide personal information via credit cards, cell phones, the Internet, and other media through a corporate third-party intermediary is not a viable option.[343] Access to the Internet is critical to financial success and income mobility.[344] Thus, the use of Gmail, the iPhone call, or the purchase on Amazon cannot be characterized as voluntary; rather, they are necessary to taking part and attaining success in society.[345] Similarly, Facebook, Twitter, cell phones, text messaging, and email are indispensable to communicating with friends and colleagues.[346]

Moreover, the still untapped uses and analyses of data suggest it is impracticable to know what information one voluntarily discloses. Indeed, our information that is subject to data analytics and data mining might be considered "less voluntary" than our content. We do not appreciate or understand how those data might be interpreted and analyzed because the algorithm for such pattern recognition has not been created yet.[347]

Users also should not be viewed as voluntarily acceding to the disclosure of their data pursuant to the notice and consent provisions of a provider

341. Klayman v. Obama, 957 F. Supp. 2d 1, 36 (D.D.C. 2013) (citing United States v. Maynard, 615 F.3d 544, 562–63 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012)); *see also* Smith v. Obama, 24 F. Supp. 3d 1005, 1009 (D. Idaho 2014) (discussing *Klayman*), *appeal docketed*, No. 14-35555 (9th Cir. July 1, 2014).

342. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 27, at 19 ("There is no reason to believe that metadata raise fewer privacy concerns than the data they describe.").

343. A privacy industry has, however, emerged. But the costs of encryption, privacy shields, and disposable email addresses and phone numbers are substantial, prompting one author to term privacy a "luxury good." Julia Angwin, *Has Privacy Become a Luxury Good?*, N.Y. TIMES (Mar. 3, 2014), http://www.nytimes.com/2014/03/04/opinion/has-privacy-become-a-luxury-good.html.

344. *See, e.g.*, Susan P. Crawford, *The New Digital Divide*, N.Y. TIMES (Dec. 3, 2011), http://www.nytimes.com/2011/12/04/opinion/sunday/internet-access-and-the-new-divide.html.

345. *See* SCHULHOFER, *supra* note 305, at 132 (contending that the third-party doctrine cases present "in effect, the option to withdraw from normal community life").

346. *See id.* at 131 ("Once we acknowledge that electronic media have become essential for maintaining personal relationships, the decision to use them is not 'voluntary,' and those who send email have not in any meaningful sense 'chosen' to assume the risk of government spying.").

347. *Cf.* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 27, at 24–25; *id.* at 44 (explaining that "the non-obvious nature of big data's products of analysis make it all but impossible for an individual to make fine-grained privacy choices for every new situation or app").

contract.[348] Rarely will users read or comprehend the potentially thousands of privacy policies they sign that set forth the ways their data may be used.[349] And individuals are not well-positioned to negotiate with tech companies over the terms and conditions of a contract and privacy protections.[350]

In making an exception to the third-party doctrine for information conveyed through intermediaries, lower courts implicitly recognize the lack of choice or voluntariness in many modern communications.[351] But the intermediary exception also appears rooted in the content/non-content distinction, applying only to intermediaries that deliver and receive communication but do not access or analyze them.[352] Yet the ubiquity of collection and analysis of email contents, for example, calls into question the force and scope of the intermediary exception.[353] The indispensability of intermediaries to a person's communications, on the other hand, suggests a solitary and solid basis for excluding information conveyed through them from the third-party doctrine. It is not feasible to communicate without some sort of intermediary.[354]

The animating rationales of the content and intermediary exceptions to the third-party doctrine reveal that these bright lines are quite porous today. The advent of big data means that non-content information we previously thought impersonal and imprecise can provide a portrait of a person not unlike that of communications contents. And the ubiquity of technological intermediaries that store and analyze our communications data are no less necessary to our participation in society and self-expression than the third parties that have conveyed our communications without accessing and studying them. But even if we do away with the third-party doctrine, it is unclear whether the individual retains a reasonable expectation of privacy in various data under the Fourth Amendment. Such a determination requires a new conceptualization of peoples' relationship to data and the interests and protections that flow therefrom.

348. *See id.* at 38. The President's Council has criticized the notice and consent regime as "unworkable and ineffective" because it makes the individual, as opposed to the company, responsible for his privacy protection. *Id.* at 40.

349. *Id.* at 38.

350. *Id.* (characterizing the asymmetry between a user and provider as "a kind of market failure"); *see also* LANIER, *supra* note 39, at 207 (noting that "network effects" make it unlikely a user can *choose* another network once a critical mass has selected a particular network).

351. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) ("Emails must pass through an ISP's servers to reach their intended recipient. Thus, the ISP is the functional equivalent of a post office or a telephone company.").

352. *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1038 (2010) ("[T]he third-party doctrine has not been extended to intermediaries that merely send and receive contents without needing to access or analyze those communications.").

353. *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 125 n.6 (E.D.N.Y. 2011).

354. *See* Hardy, *supra* note 338.

C. THE PEOPLE'S PROPRIETARY RIGHT TO DATA

In order that people may guard their own privacy and oversee the government, we must recognize a proprietary relationship between the individual and the data that she creates. By re-conceptualizing the individual's relationship to her data, she retains her personal agency, as opposed to forfeiting her rights to the corporate avatar. Most important, because of her property interest in her data, due process considerations require that before infringing that interest through collection and analysis, the government must afford her notice and an opportunity to challenge the infringement (i.e., the surveillance).[355] To construct this notice regime, I advocate building upon proposals relating to individual ownership of digital data and automated privacy preferences.

1. Monetization of Personal Data

Jaron Lanier proposes a system in which each person is "the commercial owner of any data that can be measured from that person's state or behavior."[356] An individual may choose particular transaction and privacy policies, setting a price for the use of her data.[357] Corporate and government use of even the minutest data for a large data set and resulting predictive algorithms would occasion "nanopayments" determined by the level of contribution and value.[358]

Commercializing privacy rights may not succeed in realizing some of the Fourth Amendment's original purposes. Similar to private companies, the government would pay for the use of a person's data.[359] But rather than limiting government overreach, monetization of privacy rights might incentivize individuals' capitulation of these interests. Under any system, people may elect to consent to a government search. The promise of a financial return, however, may transform the passive citizen into an active seller, fundamentally altering the relationship between the people and the government.[360]

355. *See* Mathews v. Eldridge, 424 U.S. 319, 348 (1976); Bd. of Regents of State Colls. v. Roth, 408 U.S. 564, 569–70 (1972).

356. LANIER, *supra* note 39, at 20; *see also id.* at 245–46.

357. *Id.* at 283–84, 320. Lanier's proposal amounts to an extension of theories of privacy rooted in control over information. *See, e.g.*, U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989) (discussing privacy in terms of "the individual's control of information concerning his or her person"); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 127 (2010) (describing the privacy right as "a right to appropriate flow of personal information" (emphasis omitted)); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 24–29 (2008) (discussing the theory of privacy based on the control of personal information).

358. LANIER, *supra* note 39, at 20.

359. *Id.* at 320.

360. Lanier's price-setting scheme is less radical than it may first appear. The monetization of privacy rights bears some similarity to civil damages lawsuits for constitutional violations. The

Providing clarity and avoiding case-by-case litigation over what constitutes a reasonable expectation of privacy are two benefits of Lanier's system, attributes that Kerr suggests support the third-party doctrine.[361] But a loss of nuanced judicial determinations and systematic acceptance of a base level of government surveillance would be the cost of Lanier's approach.

2. Legislating Data Ownership

The notion of interposing the individual between the government and the third-party company as the owner of the data is not just theoretical. Fourteen states currently establish that car owners and lessees own the data that are stored and analyzed in their cars' data recorders and navigation systems.[362] Federal legislation, known as the "Driver Privacy Act," has also been introduced that makes the owner or lessee of a car the owner of any data in the car's data recorder.[363] The data might include every route driven, driving habits, and speeding.[364]

The laws prohibit the sharing of this sort of information, except in limited circumstances, absent the consent of the car owner.[365] The data would otherwise be construed under the third-party doctrine as non-content information voluntarily turned over to third parties, such as Google or the Ford Motor Company, thereby negating any Fourth Amendment expectation of privacy by the driver. But the delineation of personal ownership rights, with limits on its dissemination to others, should establish an individual's reasonable expectation of privacy in those data from the government.

3. Automated Privacy Preferences

Because of the proliferation of Internet-related devices and their privacy policies' inscrutability, individuals cannot effectively control how private companies collect and use their data.[366] Transparency and user education are critical to ensuring that individuals understand what corporations do with their data. The President's Council of Advisors on Science and Technology has proposed that intermediary (yet another third party, now a fourth party)

Framers envisioned that the government-limiting objectives of the Fourth Amendment would be realized through jury trial for trespass claims. *See* Ku, *supra* note 281, at 1338–39; *supra* Part V.C.1; *supra* note 285 and accompanying text.

361. *See* Kerr, *supra* note 4, at 581–86.

362. Brian Naylor, *Putting the Brake on Who Can See Your Car's Data Trail*, NPR (Jan. 22, 2014, 4:29 PM), http://www.npr.org/blogs/alltechconsidered/2014/01/22/264996671/putting-the-brake-on-who-can-see-your-cars-data-trail.

363. Driver Privacy Act, S. 1925, 113th Cong. (2014); *see also TLJ Analysis of S 1925, the Driver Privacy Act*, TECH L.J. (Apr. 9, 2014), http://www.techlawjournal.com/topstories/2014/04 09b.asp (raising concerns over the exception's lack of requirements concerning court authorization of data retrieval, such as particularity and specificity of warrants).

364. Naylor, *supra* note 362.

365. *Id.*

366. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 27, at 38, 40.

organizations might offer "privacy preference profiles" with which individuals align.[367] The intermediary groups, such as the American Civil Liberties Union or *Consumer Reports*, would vet tech companies and their products' privacy policies for protections of their particular interests, be they civil liberties or economic value.[368]

Technological advancements may allow for an automated review of privacy policies, ensuring that individuals only choose products and services that comport with their privacy preference profiles.[369] Such widespread and automated advocacy is more likely to shift companies' privacy policies so that they comport with these profiles.[370]

4. Automated Big Data Popular Notice Regime

In the big data era, an individual cannot know all the data that private corporations and the government have and what they do with it. Lessig therefore concludes that "architecture must enable machine-to-machine negotiations about privacy so that individuals can instruct their machines about the privacy they want to protect."[371]

Building on Lanier's monetization of privacy rights and the privacy preference profiles of the President's Council may better realize the populist, government-limiting objectives of the Fourth Amendment. Rather than attaching a financial component to the data, I propose a regime in which individuals would instead select in advance whether to receive notice when the government requests their data from a third-party company. Instead of setting a price for the data, an individual would choose what forms of data collection and analysis would require notice.

The best route toward clarifying what data surveillance requires notice to the individual user is through legislation. As the driver data ownership laws suggest,[372] Congress may decide what data merit a proprietary relationship and, therefore, privacy protection. But any data about which Congress finds that surveillance would implicate privacy concerns should require notice to the individual, a cause of action for the individual, and limits on immunity afforded tech companies. Even with congressional action, however,

367. *Id.* at 40–41.

368. *Id.*

369. *Id.* at 41. The envisioned process would require "formalisms to specify privacy policies and tools to analyze software to determine conformance to those policies," as well as expressive policies and tests of adherence. *Id.*

370. *Id.* ("To attract market share, providers (especially smaller ones) could seek to qualify their offerings in as many privacy-preference profiles, offered by as many different third parties, as they deem feasible.").

371. LESSIG, *supra* note 7, at 232; *see also* LANIER, *supra* note 39, at 362 ("[E]conomics must become more and more about the design of the machines that mediate human social behavior.").

372. *See supra* Part VI.C.2.

unaddressed instances will arise that call into question whether the government may obtain a person's data.

A person's notice profile would permit an individual selection of only corporations' services and devices that provide notice to the user upon government requests for their data. A person might not want notice of every request. An individual may deem inoffensive the collection of telephony metadata for purposes of aggregate analysis and not request notice before such collection. The collection of CSLI, on the other hand, might induce concern and prompt a notice preference. Because, however, there may be forms of data analysis, with resulting revelations about personal behavior or conduct, that have yet to be discovered, general categories of data and analysis should be included within a person's notice profile.

Even without judicial or congressional endorsement of notice profiles, the market could precipitate a move toward increased notice to the individual user. As with general privacy preferences concerning the sale of one's data to particular private entities, individual preferences for notice could serve as an adjunct to limiting government surveillance by prompting companies to provide such notice to the users.

Notice also might be facilitated through future technological developments such as Lanier's proposed "Nelsonian network"—a two-way system that would record the provenance of all data.[373] The government would know in advance when a person wants notice and the person would receive notice each time the government seeks her data.[374]

These sorts of "machine-to-machine" communication of individual preferences would permit the government to decide whether it would fight for the acquisition of that specific individual's data or whether the lack of the information would not impair its investigation. If the government believes the data are necessary, it would have two options: (1) provide notice to the user and, in the event of the user's opposition (or the company's), litigate the data acquisition in court; or (2) seek a warrant from the court authorizing the surveillance without notice.

Courts may be burdened by more litigation brought by individual users over government requests for their data. But statutory clarity through legislation such as the Driver Privacy Act should guide the Executive and Judicial branches in determining what level of protection particular kinds of data require. Increased litigation is, however, the necessary cost of reinserting the individual in the conversation and negotiation with the government over her data. The Fourth Amendment must be first and foremost the people's right against unreasonable searches and seizures, not the right of the corporation.

373. LANIER, *supra* note 39, at 227.

374. *Id.*

VII. CONCLUSION

The viability of corporate avatars as an answer to the third-party doctrine's flaws nears a crossroads. The 2014 term witnessed the Supreme Court's growing recognition of privacy's fragility in the big data era and its continuing expansion of corporations' rights. In *Riley v. California*, the Court acknowledged big data's encroachment on the Fourth Amendment, holding that a cell phone search required a warrant due to the phone's vast trove of data and the intimate details that information might reveal.[375] In *Burwell v. Hobby Lobby Stores, Inc.*, the Court gave further scope to corporate rights, holding that the government's contraceptive mandate impermissibly burdened a corporation's free exercise of religion.[376]

The two lines of cases may ultimately intersect or collide. The Court will have to confront corporate avatars and their legitimacy as guardians of the Fourth Amendment. A more robust corporate Fourth Amendment right might appear to strengthen corporations' ability to resist government requests for user data. The purpose of extending a constitutional right to a corporation is, after all, as the *Hobby Lobby* majority held, to protect the rights of its people, its members.[377] But the many practical reasons set forth in this Article suggest corporations are unlikely and unable to effectively challenge the government in the majority of requests for their users' data. Moreover, the Bill of Rights' populist origins and the Framers' distrust of corporate power militate against the maintenance of the corporate avatar dynamic. Government surveillance and use of big data will increasingly implicate an individual's Fourth Amendment right, requiring that she be permitted to challenge the government.

To achieve the Fourth Amendment's privacy and government oversight objectives, individuals should normally receive notice of government surveillance and acquisition of their data. Notice may be justified on a number of grounds. First, the third-party doctrine should be limited to allow for Fourth Amendment protection of non-content data and data that are now indispensable to participate in society. Second, people should be afforded a proprietary right in much of their data. Congress may extend that right to various data, attaching to that right notice, as well as limits on incentives for corporate acquiescence to government requests for individuals' data. Finally, people may communicate their desired privacy and notice to both corporations and government through machine-to-machine technology, affording some level of ex ante clarity to the government for surveillance and pushing corporations to comport with individuals' preferences. By so

375. Riley v. California, 134 S. Ct. 2473, 2494–95 (2014).

376. Burwell v. Hobby Lobby Stores, Inc., 134 S. Ct. 2751, 2785 (2014).

377. *Id.* at 2768.

restoring agency to individuals in their relationship with the government, the Fourth Amendment can become again "[t]he right of the people."[378]

378. U.S. CONST. amend. IV.