MODERN STATE ACTION DOCTRINE IN THE AGE OF BIG DATA

*DANIEL RUDOFSKY**

TABLE OF CONTENTS

* J.D., 2016, New York University School of Law; B.A., 2011, University of Pennsylvania. I would like to thank Professors Ira Rubinstein and Katherine Strandburg for their help in the development of this Note. Thanks also to the Editors of the Annual Survey of American Law for their constructive criticism and valuable feedback.

I.
INTRODUCTION

More people than ever are concerned about their privacy online,[1] and these fears have spread to primetime television.[2] For years, academics and journalists have warned of the dangers of government's access to big data.[3] While the public has not previously been especially concerned, in the months following the Snowden revelations there was a growing outcry for action to prevent government spying.[4] Left out of much of this conversation is the role that corporations play in using their customers' data to provide their web services. The traditional line between government, which seeks to use data for law enforcement and national security purposes, and corporations, which seek to provide services to their users, has become muddled. This Note challenges the traditional distinction between government and private companies and argues that corporations should, whether required by constitutional law or the marketplace, adopt due process protections when using their users' data.

Over the past few years, companies have pushed back, even if only slightly, against alleged privacy invasions by the federal government. However, when compared to how these companies handle their own internal privacy, their resistance can appear to be only a false indication of their respect for their users' data. Instead, these companies ought to protect their data to the same degree to which they are seeking to hold the federal government.

For many Americans, George Orwell's novel *1984* is their first introduction in school to privacy.[5] In *1984*, Orwell paints a picture of the all-knowing and all-seeing government, which has its hands in and eyes on everyday life.[6] Orwell's world is an illustration of the most intrusive invasion of privacy imaginable. Compared to this world, any lesser invasion appears almost acceptable. In fact, many

1. "52% describe themselves as 'very concerned' or 'somewhat concerned' about government surveillance of Americans' data and electronic communications, compared with 46% who describe themselves as 'not very concerned' or 'not at all concerned' about the surveillance." Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RESEARCH CTR. (Mar. 16, 2015), http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden/.

2. *See Parks & Recreation: GryzzlBox* (NBC television broadcast Jan. 27, 2015).

3. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1210–12 (2004).

4. Editorial, *Edward Snowden, Whistle Blower,* N.Y. TIMES (Jan. 1 2014), http://www.nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html.

5. GEORGE ORWELL, 1984 (Alfred A. Knopf, Inc. 1992) (1949).

6. *Id.*

Americans often respond to questions about their personal privacy with a statement that they have nothing to hide.[7]

These nonchalant statements translate into practice. Today, individuals in the United States are willing to turn over a strikingly large amount of information about themselves to third-party Internet sites.[8] These same individuals would likely not want to turn over the same information to the federal government.[9] Yet the Supreme Court has held that the government can request, through subpoena, information provided to a third party without a neutral magistrate to examine *ex ante* whether there is sufficient information to allow for such an invasion.[10] This doctrine developed at least ten years prior to the invention of the World Wide Web and today's multibillion-dollar Internet companies.[11] In addition, even without this doctrine, many government agencies can purchase information from commercially available databases to provide a more complete online profile of an individual.[12] These data brokers (or fourth parties) voluntarily purchase the information from third parties, such as Google and Yahoo, which in turn collect the information from their own users.[13] This has functioned as a workaround for govern-

7. *See* Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 747 (2007).

8. *See, e.g.*, *About Facebook*, FACEBOOK, https://www.facebook.com/about/ (last visited Apr. 13, 2016) (discussing ways that individuals can provide their birthday, pictures, interests, and friends to other users).

9. *See, e.g.*, Russell Berman, *Republicans Try To Curtail the Census*, THE ATLANTIC (June 9, 2015), http://www.theatlantic.com/politics/archive/2015/06/republicans-try-to-rein-in-the-census-bureau/395210/ (reporting that Republicans sought to cut funding to the U.S. Census Bureau by preventing enforcement of criminal penalties against individuals who fail to participate in the privacy-invasive American Community Survey).

10. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

11. The World Wide Web, the protocol on which many websites are built, was first created by Sir Tim Berners-Lee in 1989, *History of the Web*, WORLD WIDE WEB FOUND., http://webfoundation.org/about/vision/history-of-the-web/ (last visited Apr. 7, 2015), a full 10 years after the Court in *Smith v. Maryland* held that information turned over to a third party has no legitimate expectation of privacy.

12. *See, e.g.*, Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 595–96 (2004) (describing commercial databases used by law enforcement to gather personal information).

13. Joshua L. Simmons, *Buying You: The Government's Use of Fourth-Parties To Launder Data About "The People,"* 2009 COLUM. BUS. L. REV. 950, 954 (2009).

ment, since the data gathered by the fourth parties is data accessible by the public.[14]

As a marketing and good will tactic, companies have often resisted government requests for data, stepping into the data protection void. Often, companies see an opportunity to fight against the government when they receive a warrant or subpoena and to insert themselves into the privacy debate. First, in pushing back against the government, they are creating independent silos by which they have complete control over data and privacy.[15] Second, they are creating precedential constitutional law by deciding in which cases to challenge the government intrusion.[16] By examining a corporation's rhetoric and theories for challenging government subpoenas and warrants, this Note tries to determine when corporations believe that they should challenge the government action.

However, that does not provide the entire answer about what corporations are doing to protect a user's privacy. While the exposure of data to law enforcement or national security agencies can bring with it a loss of liberty, there are also harms associated with the loss of privacy within a corporation's ecosystem. Internet companies claim to protect their users' rights, but how much of this is mere rhetoric, and how much are they actually protecting those rights?

There are procedural safeguards in place to protect data from unlawful government search and seizure.[17] There are not necessarily the same protections from a Google employee. The current penalties for companies may not be sufficient to encourage them to implement privacy safeguards. As companies continue to amass data in their own ecosystems, there must be incentives for them to protect privacy both internally and externally against any government intrusion.

---

14. *Id.* at 965.

15. *See infra* Part III.

16. *See, e.g.*, APPLE, REPORT ON GOVERNMENT INFORMATION REQUESTS JULY 1–DECEMBER 31, 2014, at 3 (2014), https://www.apple.com/privacy/docs/government-information-requests-20141231.pdf (Apple only produces data 79% of the time including 72% for subpoenas and 84% for warrants, and initiates legal challenges in some of those actions).

17. *See* U.S. CONST. amend. XIV, § 1 ("No state . . . shall . . . deprive any person of life, liberty, or property, without due process of law."); U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

Part I will examine the current theoretical framework by which to assess corporate efforts to protect privacy and how their duties compare to the U.S. federal government. Part II will examine whether these tech companies can be considered state actors under the state action doctrine, which would require them to abide by due process protections. Part III will conduct case studies of individual companies to examine their actions in fighting against the government and whether such companies can be considered state actors. Finally, Part IV will propose that companies adopt constitutional-equivalent due process standards, regardless of whether they are required by law, to protect a company's users from unwarranted searches and censure.

II.
CORPORATE PRIVACY HARMS

Microsoft, through its Skype application, provides users with the ability to video chat with individuals around the world,[18] Amazon allows users to buy almost anything available anywhere,[19] and Facebook assists users in keeping tabs on all their friends.[20] Each of these services works best within the networks of these companies. They have attempted to extend their ecosystems beyond their webpages through the purchase of services or creation of affiliate networks. A central question in determining the level of privacy that users should ask is: "Who governs these webpages?"

The answer is not always clear. These ecosystems are primarily governed by private law, as typically spelled out in the terms and conditions. Federal and state governments, however, may also have some authority, subject to either a subpoena or judicially-approved warrant. Indeed, according to one law professor, "[g]overnance is the product of an interlocking web of actors, both governmental and 'private,' that defines how citizens live their lives and the expectations society has regarding any specific field or topic."[21] As companies collect vast amounts of data, the companies act as sovereigns in governing most interactions within those ecosystems. The privacy policy and terms of service become the rules by which the corporation expects its actions to be judged. Furthermore, corporations have adopted interpretations of various privacy statutes that have

18. SKYPE, http://www.skype.com/ (last visited Mar. 24, 2015).

19. AMAZON, http://www.amazon.com/ (last visited Mar. 24, 2015).

20. FACEBOOK, http://www.facebook.com/ (last visited Mar. 24, 2015).

21. Marcy E. Peek, *Information Privacy and Corporate Power: Towards a Re-Imagination of Information Privacy Law*, 37 SETON HALL L. REV. 127, 146 (2006).

made these statutes essentially toothless when applied to their ecosystems.[22]

These ecosystems, from which corporations can sell the user more advertising or services, allow for more profitable Internet companies. In other words, these companies all benefit from the data that users input into their systems. However, companies have taken a while to fully understand the privacy implications of controlling all of this information. To many civil libertarians, this delay has allowed companies to amass large amounts of data without the necessary safeguards in place to protect the data originator's information.[23] Since a law enforcement actor does not need to alert the target of a search,[24] it is likely that for covert investigations, a government investigator would prefer to get information from an online website or cloud computing company than from the individual him or herself. While many sites claim that they will notify users of any government request, the government investigator can often seek a gag order.[25]

Many users understand that Internet companies compile information; however, many likely feel as if they have nothing to hide from these websites.[26] Usually, a little invasive prodding can disabuse most individuals of this theory.[27] For instance, most Internet users would not want their passwords posted around the web, nor would they be interested in having their intimate, emotional e-mails shared with unintended friends. A leading privacy scholar, Daniel Solove, points out that most people are not actually afraid that their secrets will leak online or be viewed by a government agent.[28] Instead, he characterizes this argument as one that requires a balancing test between invasive security to detect terrorists versus harmless inspection of pieces of information by well-trained government agents.[29]

---

22. *Id.* at 147–51.

23. *See, e.g.*, *Gmail Privacy FAQ*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/gmail/faq.html#13d (last visited Apr. 13, 2016) (stating that Google's privacy policy is insufficient to protect users who send e-mails through Gmail).

24. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2518(3) (2012) (allowing Judges to issue *ex parte* orders which allow a government agency to search the contents of a target's emails).

25. *See generally*, Christie Barakat, *US Tech Firms Support Facebook in Gag Order Case*, ADWEEK (Aug. 11, 2014, 1:20 PM), http://www.adweek.com/socialtimes/us-tech-firms-support-facebook-government-gag-orders/202658 (discussing various companies' reactions to use of gag orders).

26. Solove, *supra* note 7, at 749–50.

27. *Id.*

28. *Id.*

29. *Id.* at 753.

Solove argues that this balancing test is actually a false choice between security and privacy.[30] Instead, he believes that privacy is "a plurality of related problems,"[31] and that "[a] privacy problem occurs when an activity by a person, business, or government entity creates harm by disrupting valuable activities of others."[32] Professor Katherine Strandburg notes that invasions of privacy can have a "potential chilling effect . . . not only . . . [on] individual privacy, but on the First Amendment rights to freedom of association and assembly."[33]

Scholars, academics, and government actors have proposed dozens of solutions to better protect the individual privacy of consumers online. These have ranged from proposed statutes[34] to stronger FTC consent decrees.[35] However, one actor often overlooked is the website performing the task of data collection.[36] Data privacy is "governed as much by corporate action and corporate decision-making as by government regulation."[37] As described below, it is often the corporation that decides when to challenge a government subpoena or warrant as being insufficient.[38] These challenges create some of the only common law on data privacy and the Fourth Amendment.

This Note will first examine the theories underlying corporations and their integration with the modern state before analyzing the role that they play in today's Internet. Many of the first corporations were created through charters of the Crown that granted political and commercial power in their domain.[39] Under modern corporate doctrine, corporations remain fictions created by the

30. *Id.* at 753–54.

31. *Id.* at 764.

32. Solove, *supra* note 7, at 758.

33. Katherine J. Strandburg, *Freedom of Association in A Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. Rev. 741, 747 (2008).

34. *See, e.g.*, White House, Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015 (2015), https://www.whitehouse/gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (detailing proposed consumer privacy protection legislation).

35. *See, e.g.*, Greg Dickenson, *Survey of Recent FTC Privacy Enforcement Actions and Developments*, 70 Bus. Law. 247, 250–51 (2014) (surveying recent FTC privacy enforcement actions and consent decrees involving companies such as Snapchat, Inc.).

36. Peek, *supra* note 21, at 136–37.

37. *Id.* at 137.

38. *See infra* Part II.

39. *See, e.g.*, Daniel Greenwood, *The Semi-Sovereign Corporation* 2 (Univ. of Utah Legal Studies Research Paper Series, Research Paper No. 05-04, 2005), http://ssrn.com/abstracts=757315.

state, but retain many rights of individuals.[40] While there are several theories underlying the modern corporation, the shareholder primacy theory, described as when "corporations operate in the interest of the shareholders and that directors owe to them a fiduciary duty," is particularly important to modern corporate theory.[41] Furthermore, according to famed economist Milton Friedman, "there is one and only one social responsibility of business—to use its resources and engage in activities designed to increase its profits so long as it stays within the rules of the game, which is to say, engages in open and free competition without deception or fraud."[42]

In furtherance of profit, corporations today are gathering and monetizing the data of their users. Many users are willing to give this information over in favor of "ease, fastness, and convenience."[43] Yet, this does not mean that corporations must abide by the same due process procedures that government actors must follow. Marcy Peek provocatively argues that "when corporations' actions have an effect on the market that resembles the effect of governmental authority and . . . that corporate authority goes largely unchallenged and is, in fact, accepted as the social norm, corporations are engaging in governance."[44] In the privacy sphere, this Note argues that corporations are governing the web.

By providing this data, a user grants a corporation a unique position to cause harm through the misuse of the user's data. For most of American history, the overriding privacy concern was a fear of government intrusion. Today, however, corporate actors have the capability, and occasionally the business need, to affect a similar harm. In some instances, the potential harm by a corporation can be even greater than the harm caused by government.

Each of the companies discussed in Part III has the ability to violate certain rights of ordinary individuals. Paul Ohm characterizes the potential harms from revealing sensitive data as ancient, traditional, and modern.[45] In the ancient basket, he places "easy-to-

40. *See, e.g.*, Citizens United v. FEC, 558 U.S. 310, 342 (2010) (stating that corporations have First Amendment rights to speak during elections).

41. Allison D. Garrett, *The Corporation as Sovereign*, 60 ME. L. REV. 129, 136 (2008).

42. Milton Friedman, *The Social Responsibility of Business Is To Increase Its Profits*, N.Y. TIMES MAG., Sept. 13, 1970, at 427 (quoting MILTON FRIEDMAN, CAPITAL AND FREEDOM 133 (Univ. of Chicago Press 1982)).

43. Lee Rainie & Janna Anderson, *The Future of Privacy*, PEW RESEARCH CTR. (Dec. 18, 2014), http://www.pewinternet.org/2014/12/18/future-of-privacy/ (quoting an information science professional).

44. Peek, *supra* note 21, at 146.

45. Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1161 (2015).

measure, if not strictly monetary, harm."[46] The traditional harms often involve injury to dignity or emotion.[47] Finally, he discusses the more controversial, modern harms, which include "losing control over one's information or defin[ing] privacy as limited access to self or for the protection of intimacy."[48]

Revealing intimate, sensitive details by either government or a corporation can lead to any of these specific harms. In addition, the use of data by those same actors in a pernicious way can produce the same result. These harms are most likely to be in the modern category, but can be found in the ancient or traditional as well. Target, in a famous example, analyzed purchase history and began advertising products for pregnant women to a young woman.[49] Her father saw the advertisements and was disgusted by Target for this advertising, only to later find out that his daughter was pregnant.[50] The daughter could be a candidate for a lawsuit against Target for an infliction of emotional damage. While there is no indication an employee sought to blackmail the daughter, one could imagine a scenario in which an employee at Target used the company's algorithm to perform a background check on a potential date or business partner.

III.
CONSTITUTIONAL RIGHTS

A. First and Fourth Amendment Rights

The First and Fourth Amendments have been construed to provide a right to privacy for Americans.[51] Justice Brandeis, in his oft-quoted dissenting opinion in *Olmstead v. United States*, said, "[The founders] sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the *right to be let alone*—the most comprehensive of rights and the right most valued by civilized men."[52] This dissent is the birthplace of most of constitutional privacy law, and the Supreme Court's later decisions have incorporated this right of

46. *Id.* at 1162.

47. *Id.* at 1163.

48. *Id.* at 1164.

49. Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES MAG., Feb. 19, 2012, at 30–37, 54–55.

50. *Id.* at 37.

51. Griswold v. Connecticut, 381 U.S. 438, 484 (1965) ("Various [amendments] create zones of privacy.").

52. Olmstead v. United States, 277 US 438, 478 (1928) (Brandeis, J., dissenting) (emphasis added).

privacy against the states.[53] Our founders may have fought against the tyranny of Great Britain, but they certainly weren't aware of the potential harm of all-knowing Internet companies.

But what do these two Amendments *actually protect*? It is well-established that the government cannot censor the opinions of average citizens.[54] This is a bedrock principle of First Amendment law. In addition, the First Amendment protects the right of citizens to engage in an open forum with their peers to discuss ideas that may be harmful to the government.[55] In *Perry Educational Ass'n v. Perry Local Educators Ass'n*, the Court distinguished between three types of public fora: streets and parks, "public property which the state has opened for use by the public as a place for expressive activity," and property to which the state, through tradition or designation, has not recognized as a "forum for public communication."[56] The first two types of public fora, traditional and designated, are subject to the highest scrutiny, and "[f]or the state to enforce a content-based exclusion it must show that its regulation is necessary to serve a compelling state interest and that it is narrowly drawn to

53. The First Amendment's freedom of speech was first incorporated against the states in *Gitlow v. New York*, 268 U.S. 652, 666 (1925). Gitlow includes suggested language that assumes that the First Amendment applies against the state. *Id.* ("For present purposes we may and do assume that freedom of speech and of the press . . . are among the fundamental personal rights and 'liberties' protected by the due process clause of the Fourteenth Amendment from impairment by the States."). Along with freedom of speech, the Freedom of Assembly Clause was incorporated against the states in *De Jonge v. Oregon*, 299 U.S. 353, 364 (1937). And the freedom to associate was first found in the First Amendment and incorporated against the states in *NAACP v. Alabama*, 357 U.S. 449, 462 (1958) ("We think that the production order, in the respects here drawn in question, must be regarded as entailing the likelihood of a substantial restraint upon the exercise by petitioner's members of their right to freedom of association."). The Fourth Amendment's provision requiring individuals to be free from unreasonable search and seizure was first applied against the states in *Wolf v. Colorado*, 338 U.S. 25, 28 (1949) ("Accordingly, we have no hesitation in saying that were a State affirmatively to sanction such police incursion into privacy it would run counter to the guaranty of the Fourteenth Amendment."), *overruled on other grounds by* Mapp v. Ohio, 367 U.S. 643 (1961).

54. Citizens United v. FEC, 558 U.S. 310, 340–41 (2010) ("Premised on mistrust of governmental power, the First Amendment stands against attempts to disfavor certain subjects or viewpoints."). There are limited exceptions to this rule that are "based on an interest in allowing governmental entities to perform their functions." *Id.* at 341.

55. Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45 (1983) ("In places which by long tradition or by government fiat have been devoted to assembly and debate, the rights of the state to limit expressive activity are sharply circumscribed.").

56. *Id.* at 45–47.

achieve that end."[57] The final type of forum is not subject to these same strict scrutiny requirements.[58]

In *Reno v. ACLU*, the Court first examined whether the Internet is entitled to a different, perhaps relaxed, First Amendment protection.[59] The Court found that the Internet does not present any reason for the government to be held to a lower standard of First Amendment protection.[60] In a recent Fourth Circuit case concerning the extent of speech, a panel held that even liking a Facebook page qualifies as constitutionally protected speech.[61]

The harder cases are those that challenge a governmental action on the grounds that it chills the freedom of association or speech.[62] In *Clapper v. Amnesty International*, the Court examined whether Amnesty International had standing to challenge the constitutionality of the FISA Amendments Act.[63] As part of this analysis, Amnesty International claimed that the government's acquisition of membership data could chill its First Amendment rights.[64] The Court said that a "chilling effect aris[ing] merely from the individual's knowledge that a governmental agency was engaged in certain activities or from the individual's concomitant fear that, armed with the fruits of those activities, the agency might in the future take some *other* and additional action detrimental to that individual" was not sufficient to plead a First Amendment violation.[65]

It is also well established that the Fourth Amendment protects Americans from "unreasonable searches and seizure" of their "persons, houses, papers, and effects,"[66] and that this right applies to

57. *Id.* at 45.

58. *Id.* at 46.

59. Reno v. ACLU, 521 U.S. 844, 870 (holding that the Communications Decency Act, which sought to prevent children from looking at explicit pictures on the Internet, was overbroad and was a facially unconstitutional imposition on First Amendment rights).

60. *Id.*

61. *See, e.g.*, Bland v. Roberts, 730 F.3d 368, 386 ("Once one understands the nature of what Carter did by liking the Campaign Page, it becomes apparent that his conduct qualifies as speech.").

62. *See generally* Katherine J. Strandburg, *Membership Lists, Metadata, and Freedom of Association's Specificity Requirement*, 10 I/S: J. L. & POL'Y FOR INFO. SOC'Y. 327 (2014) (examining the legality of the NSA surveillance program in light of the freedom of association).

63. Clapper v. Amnesty Int'l, 133 S.Ct. 1138 (2013).

64. *Id.* at 1152.

65. *Id.* (quoting Laird v. Tatum, 408 U.S. 1, 11 (1972)).

66. U.S. CONST. amend. IV.

computers and other digital effects.[67] The Supreme Court has held that a search violates the Fourth Amendment when "the government violates a subjective expectation of privacy that society recognizes as reasonable."[68] However, the Court has yet to examine whether a warrant is required for searches of content on the Internet. The Sixth Circuit in *United States v. Warshak* held "that a subscriber enjoys a reasonable expectation of privacy in the contents of e-mails 'that are stored with, or sent or received through, a commercial ISP.'"[69]

In addition, the Supreme Court has found certain exceptions to this general warrant requirement. The most prominent exception in the Internet age is the third-party doctrine. This doctrine was best articulated in *Smith v. Maryland*, in which the Court held that records voluntarily given to a third party can be requested without a warrant.[70] In the Supreme Court's *Jones* decision, at least one Justice suggested the Court should rethink the third-party doctrine.[71] Finally, in *Riley v. California*, the Court held that police could not search a phone gathered incident to an arrest because "[w]ith all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'"[72] It is not clear if the Court is beginning to rethink the third-party doctrine or if it is willing to recognize that people have some privacy interest in information online. At the moment, the Court's Internet privacy cases are in their infancy, but it seems likely that the Court is beginning to question its current doctrine in light of technological advances such as cloud computing and smart phones.

---

67. *See generally* Orin S. Kerr, 119 HARV. L. REV. 531, *Searches and Seizures in A Digital World* 549 (2005) ("[T]he Fourth Amendment applies to computer storage devices just as it does to any other private property.").

68. United States v. Jones, 132 S. Ct. 945, 954–55 (2012) (Sotomayor, J., concurring) (*citing* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

69. United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010) (quoting Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007)).

70. Smith v. Maryland, 442 U.S. at 743–44 ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

71. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (stating that the third-party doctrine is "ill suited [sic] to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks").

72. Riley v. California, 134 S. Ct. 2473, 2494–95 (2014) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

B. State Action Doctrine

While courts have held that private corporations are not subject to the restrictions of the Bill of Rights or the Fourteenth Amendment, the advent of Internet ecosystems has further intertwined private corporations with the traditional role of the government. Some early Internet users sought to make the case that operators of online ecosystems are state actors for purposes of the Fourteenth Amendment's Due Process Clause and are therefore responsible for the violation of constitutional rights.[73] They sought to analogize the idea that Internet forums have literally and figuratively displaced the public street corner or park as the location of debate.[74]

However, the State Action Doctrine is based on a textual understanding of the Constitution.[75] The Fourteenth Amendment states, "No State shall make or enforce any law,"[76] while the First Amendment says that "Congress shall make no law."[77] Furthermore, the Constitution reserves rights that are not explicitly delegated to the United States to the states or to the people.[78] This means that private actors are free to transgress the freedom of speech and privacy rights found in the Constitution subject to only some more stringent state constitutional restrictions.[79] Currently, the marketplace likely dictates an open web, but there are often scenarios that occur in which Internet companies clamp down on speech.[80]

---

73. *See, e.g.*, Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 436, 445 (E.D. Pa. 1996) ("In sum, we find that since AOL is not a state actor and there has been no state action by AOL's activities under any of the three tests for state action . . . .").

74. *See* Jacquelyn E. Fradette, Note, *Online Terms of Service: A Shield for First Amendment Scrutiny of Government Action*, 89 NOTRE DAME L. REV. 947, 956–57 (2013).

75. *See* Wilson R. Huhn, *The State Action Doctrine and the Principle of Democratic Choice*, 34 HOFSTRA L. REV. 1379, 1387, 1430–31 (2006).

76. U.S. CONST. amend. XIV.

77. U.S. CONST. amend. I.

78. U.S. CONST. amend. X.

79. *See, e.g.*, Pruneyard Shopping Ctr. v. Robins, 447 U.S. 74, 81 (1980) (holding that a state can exercise its police power or sovereign right to adopt more expansive rights than those in the Bill of Rights).

80. *See* Julia Greenberg, *Reddit Wants To Exile Trolls. But Growing Up Is Hard*, WIRED (May 15, 2015, 7:00 AM), http://www.wired.com/2015/05/reddit-wants-exile-trolls-growing-hard/ (reporting that a popular social media site banned harassing language).

The Supreme Court has developed a lengthy case law in this area that some describe as muddled and incoherent.[81] In the furthest-reaching of its decisions on the state action principle, *Shelley v. Kraemer,* the Court held that a state court enforcing a private housing covenant was a form of state action and therefore the discriminatory housing covenant could not be enforced by the state.[82] It did not find that the discriminatory covenant itself violated the Fourteenth Amendment since there was no state actor.[83] In the years since *Shelley*, the Court has moved away from treating all court enforcement, federal or state, as state action.[84] Otherwise, private corporations could not enter into agreements that might abridge the freedom of speech or other constitutional rights of their citizens because these agreements require court supervision for enforcement.

The most recent Supreme Court case, *Brentwood Academy v. Tennessee Secondary School Athletic Ass'n*, found "state action may be found if, though only if, there is such a 'close nexus between the State and the challenged action' that seemingly private behavior 'may be fairly treated as that of the State itself.' "[85] The Court used a totality of the circumstances test to determine that the athletic association was a state actor.[86] The Court outlined certain factors to be considered, including when the action "results from the State's exercise of 'coercive power,' when the State provides 'significant en-

81. *See* Gary Peller & Mark Tushnet, *State Action and a New Birth of Freedom*, 92 GEO. L.J. 779, 789 (2004) ("The state action doctrine is analytically incoherent because . . . state regulation of so-called private conduct is always present, as a matter of analytic necessity, within a legal order.").

82. Shelley v. Kraemer, 334 U.S. 1, 20 (1948) ("We hold that in granting judicial enforcement of the restrictive agreements in these cases, the States have denied petitioners the equal protection of the laws and that, therefore, the action of the state courts cannot stand.").

83. *Id.* at 13 ("We conclude, therefore, that the restrictive agreements standing alone cannot be regarded as a violation of any rights guaranteed to petitioners by the Fourteenth Amendment.").

84. *See* Lugar v. Edmondson Oil Co., Inc., 457 U.S. 922, 939 n. 21 (1982) ("[W]e do not hold today that 'a private party's mere invocation of state legal procedures constitutes "joint participation" or "conspiracy" with state officials satisfying the § 1983 requirement of action under color of law.' " (quoting *id.* at 951) (Powell, J., dissenting)). *Lugar* is a case in which Edmondson Oil attempted to take possession of Lugar's truck stop after Edmondson claimed that Lugar owed the company money. Edmondson used the state sheriff and the court system to take possession. Lugar sued Edmondson under 42 U.S.C. § 1983 accusing Edmondson of violating his property rights without due process. *Id.*

85. Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n, 531 U.S. 288, 295 (2001) (quoting Jackson v. Metro. Edison Co., 419 U.S. 345, 351).

86. *Id.* at 295–96.

couragement, either overt or covert,' or when a private actor operates as a 'willful participant in joint activity with the State or its agents.' "[87] Furthermore, the Court "ha[s] treated a nominally private entity as a state actor when it is controlled by an 'agency of the State,' when it has been delegated a public function by the State, when it is 'entwined with governmental policies,' or when government is 'entwined in [its] management or control.' "[88]

This totality of the circumstances test stands in stark contrast to a rules-based approach advocated in earlier Court decisions. In *Blum v. Yaretsky,* the Court runs through three factors and finds that the petitioner is unable to meet the burden to show that a nursing home is a state actor.[89] The factors are whether (1) "there is a sufficient nexus between the State and the challenged action of the regulated entity so that the action of the latter may be fairly treated as that of the State itself,"[90] (2) a state has "exercised coercive power,"[91] or (3) a "private entity has exercised powers that are 'traditionally the exclusive prerogative of the State.' "[92]

According to one commentator, this disagreement revolves around the purpose of the state action doctrine.[93] Chief Justice Rehnquist believed strongly in favor of a rules-oriented approach because he believed he was protecting individual liberty.[94] He notes in *DeShaney v. Winnebago County Department of Social Services* that the Due Process Clause of the Fourteenth Amendment does not "require[ ] the State to protect the life, liberty, and property of its citizens against invasion by private actors."[95]

On the other hand, liberal scholars such as Cass Sunstein argue that "state action is always present," and decisions should be based on the merits of whether someone's constitutional rights were violated.[96] Sunstein argues that in an employment decision based on a race, an employer is either allowed or not allowed to hire or not hire based on existing constitutional and statutory law.[97]

87. *Id.* at 296 (internal citations omitted).
88. *Id.* (internal citations omitted).
89. Blum v. Yaretsky, 457 U.S. 991, 1005 (1982).
90. *Id.* at 1004 (quoting *Jackson*, 419 U.S. at 350).
91. *Id.* at 1004.
92. *Id.* at 1005 (quoting *Jackson*, 419 U.S. at 353).
93. *See* Huhn, *supra* note 75, at 1392–93.
94. *Id.* at 1393.
95. DeShaney v. Winnebago Cnty. Dep't of Soc. Servs., 489 U.S. 189, 195 (1989).
96. Cass R. Sunstein, *State Action Is Always Present*, 3 CHI. J. INT'L L. 465, 467 (2002).
97. *Id.* at 468.

If the employer fires a gay person based on his sexual orientation, that employer is relying on the absence of a law specifically protecting that person.[98]

Wilson Huhn believes that both these viewpoints overstate the importance and the role of the state action clause.[99] He believes that the state action clause is meant to limit the role of the Fourteenth Amendment and force people, through their democratically elected legislatures, to determine the "kind of society they wish to live in."[100] The Framers, he argues, placed the power to regulate corporations and other non-state actors in the elected legislature, and the state action doctrine serves to prevent litigants and the judiciary from circumventing the legislature.[101]

C. Exceptions to the State Action Doctrine

Based on this current doctrine, the exemptions for when non-state actors have been found to be state actors can be grouped into two categories: "the public function exception" and the "entwinement exception."[102]

The Court first examined the public function exemption in the case of *Marsh v. Alabama*.[103] In *Marsh*, the Court found that even though a company had title to the town, its role as owner was indistinguishable from that of a municipality, and therefore the company could not violate the First Amendment rights of citizens within the town.[104] The Court, in *Jackson v. Metropolitan Edison Co.*, narrowed this exception to require "a sufficiently close nexus between the State and the challenged action of the regulated entity so that the action of the latter may be fairly treated as that of the State itself."[105] In *Lloyd v. Tanner*, the Court found that *Marsh v. Alabama* was the "closest decision in theory" and "involved the assumption by a private enterprise of all of the attributes of a state-created municipality and the exercise by that enterprise of semi-official municipal functions as a delegate of the State."[106]

---

98. *Id.*

99. *See generally* Huhn, *supra* note 75.

100. *Id. at* 1381–82.

101. *Id.*

102. Benjamin F. Jackson, *Censorship and Freedom of Expression in the Age of Facebook*, 44 N.M. L. REV. 121, 142 (2014).

103. Marsh v. Alabama, 326 U.S. 501 (1946).

104. *Id.* at 507–08.

105. Jackson v. Metro. Edison Co., 419 U.S. 345, 351 (1974).

106. Lloyd Corp., Ltd. v. Tanner, 407 U.S. 551, 569 (1972).

The entwinement exception was laid out by the Court in *Lugar v. Edmonson Oil*.[107] In *Lugar*, the plaintiff brought an 18 U.S.C. § 1983 suit against Edmonson Oil for violating his constitutional rights. Edmonson Oil had allegedly attached his property to a debt action, and therefore "had acted jointly with the State to deprive him of his property without due process of law."[108] The Court found that the test to determine whether the private actor has been entwined with the state is whether "he is a state official, . . . he has acted together with or has obtained significant aid from state officials, or . . . his conduct is otherwise chargeable to the State."[109] The Court further held that "a private party's joint participation with state officials in the seizure of disputed property is sufficient to characterize that party as a 'state actor' for purposes of the Fourteenth Amendment."[110] This was reaffirmed in *Brentwood Academy v. Tennessee Secondary School Athletic Ass'n* when the Court declared that "[t]he nominally private character of the Association is overborne by the pervasive entwinement of public institutions and public officials in its composition and workings . . . ."[111]

In either instance, it is clear that many of the Internet companies surveyed in the Electronic Frontier Foundation report share the role of government in providing the rules and regulations for their ecosystems.[112] The most likely candidates for companies that could be considered state actors are Internet Service Providers (ISPs) and Search Engines.

D. Can Internet Service Providers Be Classified as State Actors?

In several instances, individuals have sued service providers seeking to claim that service providers are state actors. In an early case in 1996, Cyber Promotions, an advertiser, sought to color actions taken by America Online (AOL) as state actions.[113] At this time, AOL operated dial-up Internet and an e-mail service that often operated as a conduit for individuals to access the World Wide Web. Cyber Promotions was attempting to send advertisements to AOL customers, and AOL prevented this unsolicited e-

107. Lugar v. Edmondson Oil Co., Inc., 457 U.S. 922, 942 (1982).

108. *Id.* at 925.

109. *Id.* at 937.

110. *Id.* at 941.

111. Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n, 531 U.S. 288, 298 (2001).

112. *See infra* Part III.

113. Cyber Promotions v. AOL, 948 F. Supp. 436, 441 (E.D. Pa. 1996).

mail access.[114] The district court held that AOL was not a state actor under three tests as determined by the Third Circuit.[115] Under the exclusive public function test, the court determined that AOL did not perform an exclusive public function, since government did not regulate the "exchange of information between people, institutions, corporations and governments around the world," and there were other avenues for people to access the Internet.[116] The Court combined the second and third tests as a form of the entwinement test and found that AOL received no direction or pressure from state officials.[117]

In another case, the Third Circuit found that AOL was also not a state actor for purposes of policing its chat rooms.[118] The plaintiff sued AOL for refusing to take action under its terms of service against several alleged chat room instigators.[119] The court found that providing a connection to government websites and opening a network to the public was not sufficient to find that AOL performed an exclusive public function.[120]

A case from Canada may provide the framework for U.S. courts to examine whether an ISP can be entwined with the functions of the state.[121] The Canadian court in *R. v. Weir* found that the ISP, by providing child pornography messages sent to the defendant, could be found to be a state agent.[122] According to two scholars, in the fight against cybercrime, ISPs are becoming state agents by notifying authorities of criminal behavior on their networks and participating in investigations.[123]

In addition, the FCC's reclassification of ISPs as common carriers may further entwine ISPs with the state.[124] According to the FCC, broadband companies must be open conduits for speech on the Internet.[125]

---

114. *Id.* at 437.
115. *Id.* at 441.
116. *Id.* at 441–43.
117. *Id.* at 444–45.
118. Green v. AOL, 318 F.3d 465, 472 (3d Cir. 2003).
119. *Id.* at 468.
120. *Id.* at 472.
121. *See* R. v. Weir (2001), 281 A.R. 333 (Can. Alta. C.A. 2001).
122. *Id.* at ¶ 11; s*ee also* Ian Kerr & Daphne Gilbert, *The Role of ISPs in the Investigation of Cybercrime*, *in* INFORMATION ETHICS IN THE ELECTRONIC AGE: CURRENT ISSUES IN AFRICA AND THE WORLD 163, 166 (Tom Mendina & Johannes J. Britz eds., 2004).
123. *See* Kerr & Gilbert, *supra* note 122, at 171.
124. Protecting and Promoting the Open Internet, *Report and Order on Remand and Declaratory Ruling and Order*, FCC 15-24, 30 FCC Rcd 17905 (2015).
125. FCC No Blocking Rule, 47 C.F.R. § 8.5 (2015).

Courts have almost uniformly found that ISPs do not provide a public function. However, recent regulatory action by the FCC may provide an opening in future cases to classify ISPs as state actors.

E. Can Search Engine Companies Be Classified as State Actors?

In *Langdon v. Google,*[126] the plaintiff alleged in a § 1983 suit that Google violated his First Amendment rights by refusing to run political ads and ranking the plaintiff's website low on its search results. The court found that Google is a "private, for profit company, not subject to constitutional free speech guarantees."[127] The plaintiff alleged two theories about why Google should be considered a state actor.[128] The first was that Google was entwined with public universities, and the second was that Google was similar to private shopping centers.[129] The court found that the plaintiff failed to allege facts that would prove that there was entwinement and that the Supreme Court had consistently found that private shopping centers are not public forums protected by the First Amendment.[130] This case is representative of "the attitude of courts regarding attempts to enforce First Amendment duties on Internet Service providers."[131]

These cases illustrate that courts that have examined this issue have consistently found that websites are not public actors for purposes of the Fourteenth Amendment. However, as these companies build extensive databases on individuals, courts may become more receptive to examining these actors as state actors.

F. Current NSA Law and Encryption Debate

President Obama recently signed into law a bill to reform the NSA spying apparatus.[132] The law now requires phone companies to produce specific records of individuals and prohibits the NSA

126. Langdon v. Google, Inc., 474 F. Supp. 2d 622, 626 (D. Del. 2007).

127. *Id.* at 631.

128. *Id.* at 631–32.

129. *Id.*

130. *Id.*

131. Gil'ad Idisis, *How to Make Lemonade from Lemons: Achieving Better Free Speech Protection Without Altering the Existing Legal Protection for Censorship in Cyberspace*, 36 CAMPBELL L. REV. 147, 167 (2013).

132. *See* Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015).

from the bulk collection of such information.[133] In replacing the NSA's ability to bulk collect such information, the burden to store the same information and provide it to the government, subject to certain specific processes, falls to Internet companies.[134] These companies currently keep the same information for anywhere from eighteen months to five years.[135] This has been deemed front-door access since the government is asking, pursuant to an ex parte Foreign Intelligence Surveillance Court (FISA Court) order, for the entity for this data.[136] The law also contains a safe harbor for companies that provide the information to the government in good faith.[137] This further entwines the government and the private corporation against the potential best interests of the customer.

The government has also sought to ensure backdoor access to data stored on cell phones.[138] Apple, Google, and many other companies have sought to secure information on their devices from both government spies and potential hackers.[139] These conflicting interests escalated in the first quarter of 2016 when the debate spilled out of the courtroom.[140] The federal government sought to access the information on an iPhone owned by a mass shooter.[141] Apple responded in court and online to its millions of customers.[142] While the FBI was able to access the cell phone through a third

133. Jodie Liu, *So What Does the USA Freedom Act Do Anyway?*, LAWFARE (June 3, 2015, 5:29 PM), https://www.lawfareblog.com/so-what-does-usa-freedom-act-do-anyway.

134. 50 U.S.C.A. § 1861(a) (West 2016).

135. Jennifer Steinhauer, *House Votes To End N.S.A.'s Bulk Phone Data Collection*, N.Y. TIMES (May 13, 2015), http://www.nytimes.com/2015/05/14/us/house-votes-to-end-nsas-bulk-phone-data-collection.html.

136. Joris V.J. van Hoboken & Ira S. Rubinstein, *Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era*, 66 ME. L. REV. 488, 514 (2014).

137. 50 U.S.C.A. § 1861(e) (West 2016).

138. Seth Schoen, *The Government Wants A Backdoor Into Your Online Communications*, ELECTRONIC FRONTIER FOUND. (May 22, 2003), https://www.eff.org/deeplinks/2013/05/caleatwo.

139. Devlin Barrett, Danny Yadron & Daisuke Wakabayashi, *Apple and Others Encrypt Phones, Fueling Government Standoff*, WALL ST. J. (Nov. 19, 2014, 10:30 PM), http://www.wsj.com/articles/apple-and-others-encrypt-phones-fueling-government-standoff-1416367801.

140. *See* Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/.

141. Timothy Lee, *Apple's Battle with the FBI over iPhone Security, Explained*, VOX (Feb. 17, 2016, 3:50 PM), http://www.vox.com/2016/2/17/11037748/fbi-apple-san-bernardino.

142. *Id.*

party,[143] it is clear that this debate is not over and that Apple believes that it is worth challenging the government and a leading Presidential candidate over the security of its devices.[144]

IV.
CASE STUDIES OF SELECT INTERNET-RELATED COMPANIES

This Part applies the principles of the state action doctrine to those companies that have challenged government action. It will seek to show that these actors are, in fact, performing traditional governmental actions online.

There are two general reasons why a website may seek to encroach upon a user's rights.[145] The first is because of an external power requesting the deprivation.[146] The second is because of internal pressures, such as seeking to protect a site's users from dangerous criminals, pornographic materials, hacking, and copyright violations.[147] Many websites have begun to publish statistics, in biannual transparency reports, on instances in which they have fought against the external pressure; however, there is quite a lack of transparency in how these websites handle various internal pressures.

The Electronic Frontier Foundation (EFF), a non-profit dedicated to being an independent watchdog to protect Internet users,[148] has spent years pressuring companies and the United States government to improve their privacy protections. The EFF releases an annual report grading the efforts of Internet companies

143. Katie Benner & Eric Lictblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. TIMES (Mar. 28, 2016), http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html.

144. *See* Lindsey J. Smith, *Donald Trump on Apple Encryption Battle: "Who Do They Think They Are?,"* VERGE (Feb. 17, 2016, 11:53 AM), http://www.theverge.com/2016/2/17/11031910/donald-trump-apple-encryption-backdoor-statement (describing Donald Trump's view that the government must develop tools to break encryption technology in order to protect American's from terrorism).

145. *See* Jackson, *supra* note 102, at 127–32 (discussing the reasons a website might engage in censorship).

146. *Id.* at 127–29.

147. *Id.* at 129–31.

148. "Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development." *About*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/about (last visited Feb. 11, 2015).

to fight against government intrusions into privacy.[149] Through this list of Internet corporations, I attempted to find each of the instances in which a company fought against a government subpoena and for which the records are publicly available. Where I could not find the actual case, I sought to use the EFF's own record or a statement from the company. Unfortunately, many of these cases are sealed by court order and are therefore not available.

Through an examination of each of the thirteen companies that gets a star in the EFF's 2014 report, this Note seeks to describe how each company gathers data, uses data, responds to external requests for the data, and finally, responds to internal data invasions. The Note expands on the EFF report by seeking to provide context for each company's policies and actions. All of these companies must be applauded for taking the government to court in the instances detailed below. Occasionally, there seems to be another motive beyond the privacy of their users. Regardless of the primary motive, all of these companies have spent significant sums of money protecting the privacy of their users, which shows that at a fundamental level, user privacy is important to the company.

The first five companies are listed according to their market capitalization.[150] These companies are most likely to be considered state actors because of their size. The rest are then listed in alphabetical order.

A. Apple

Apple, first incorporated in 1976, was originally a personal computing company.[151] It has since dominated the music industry with the iPod and iTunes, created the tablet industry with the iPad, and shaken up the smart phone industry with the iPhone. Many consumers spend their entire days at work and home within the

149. Nate Cardozo et. al., *Who Has Your Back? Protecting Your Data from Government Requests*, ELECTRONIC FRONTIER FOUND. (May 15, 2014), https://www.eff.org/files/2014/05/15/who-has-your-back-2014-govt-data-requests.pdf.

150. As of April 28, 2016, Apple's market capitalization (market cap) is $542.37 billion, Google's market cap is $496.6 billion, Microsoft's market cap is $400.41 billion, Facebook's market cap is $390.93 billion, and Amazon's market cap is $285.6 billion. *NASDAQ Companies*, NASDAQ, http://www.nasdaq.com/screening/companies-by-industry.aspx?industry=ALL&exchange=NASDAQ&sortname=marketcap&sorttype=1 (last visited Apr. 28, 2016).

151. *The Apple Revolution: 10 Key Moments*, TIME, http://content.time.com/time/specials/packages/article/0,28804,1873486_1873491_1873530,00.html (last visited Mar. 25, 2015).

Apple ecosystem.[152] In addition, Apple is the first U.S. company to achieve a market capitalization greater than $700 billion.[153] Finally, Apple's most recent innovations may create the largest potential privacy problems. In the past several years, it has introduced ApplePay, which seeks to digitize a person's credit cards; Apple HealthKit, which centralizes health information gathered from the iPhone and its accessories; and AppleWatch, which seeks to place all the information from the iPhone onto one's wrist.[154] These new innovations allow Apple to track the physical location, purchases, health, and other intimate details of its users.

Apple has recognized the unique role that it plays in the daily lives of its users. Its current CEO, Tim Cook, explained in a recent speech at a discussion convened by President Obama that Apple sees itself as a guardian of a user's trust by providing superior privacy protections and security.[155] To this end, he said that Apple seeks to protect its users through privacy by design[156] such as segmenting networks and systems, asking users' permission to share data to improve services, and refraining from selling users' data to third parties.[157] In the same speech, he chastised governments around the world for their failure to protect the privacy of their citizens, describing the horrible damage that can be done through violating someone's most intimate details.[158] He came out strongly in favor of a right to privacy to protect "our way of life."[159]

Apple and Tim Cook have also acted on this impulse to protect their users' right to privacy by stating in Apple's transparency report, "[i]f there's a question about the legitimacy or scope of the request we challenge it, as we have done as recently as this year."[160] In addition, in an open letter to its users following publicized

152. Mat Honan, *Why Apple Devices Will Soon Rule Every Aspect of Your Life*, WIRED (Sept. 10, 2014, 6:30 AM), http://www.wired.com/2014/09/apple-ecosystem/.

153. Jennifer Booton, *Apple Valuation Could Hit $845 Billion—Or More*, MARKETWATCH (Feb. 11, 2015, 10:27 AM), http://www.marketwatch.com/story/apple-valuation-could-hit-845-billion-or-more-2015-02-11.

154. Honan, *supra* note 152.

155. Tim Cook, CEO, Apple, Address at the White House Summit on Cybersecurity and Consumer Protection at Stanford University (Feb. 13, 2015).

156. Privacy by design refers to "embedding [privacy] into the design specifications of technologies, business practices, and physical infrastructures." *Introduction to PbD*, INFO. & PRIVACY COMM'R OF ONT., https://www.ipc.on.ca/english/privacy/introduction-to-pbd/ (last visited Apr. 14, 2016).

157. Cook, *supra* note 155.

158. *Id.*

159. *Id.*

160. APPLE, *supra* note 16.

breaches of its cloud system, Tim Cook stated that Apple has "never worked with any government agency from any country to create a backdoor in any of our products or services."[161]

In a letter responding to a request for information by a court, Apple explained that it objected to at least nine requests for assistance to decrypt an iPhone and requested more information in two cases.[162] In at least two of these instances, judges allowed the information to be released publicly.[163] And in one case, the Magistrate Judge ruled against the government by finding that the government's construction of the All Writs Act, a 1787 law allowing courts to issue any writ necessary for the judiciary to carry out its duties,[164] was too broad to require Apple to provide access to a locked iPhone.[165] In another case, the Magistrate Judge ruled that Apple had to fulfill the government's request to unlock the iPhone of the San Bernardino mass shooting killer.[166] Apple refused to comply with the initial order and continued to fight against it. However, a third party was able to assist the FBI in accessing the data on the cell phone.[167]

In addition, Tim Cook's speech and Apple's biannual transparency report are further indications of how Apple approaches privacy inside its ecosystem and how it evaluates external requests. According to Apple's transparency report, it objected to seventy-five account requests out of a total of 788 for an objection rate of roughly 9.5%.[168] In roughly 80% of cases, Apple says that it provided some information to law enforcement.[169]

161. Tim Cook, *Apple's Commitment to Your Privacy,* APPLE, https://www.apple.com/privacy/ (last visited Mar. 29, 2015).

162. Letter from Apple to Orenstein, J., *In re* Order Requiring Apple Inc. To Assist in the Execution of a Search Warrant Issued by the Court, No. 15-MC-1902, 2016 WL 783565 (E.D.N.Y. Feb. 17, 2016) [hereinafter *N.Y. Search Warrant Case*], http://pdfserver.amlaw.com/nlj/apple_allwrits_list.pdf.

163. *See N.Y. Search Warrant Case*; *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-MJ-00451, 2016 WL 618401 (C.D. Cal Feb. 16, 2016) [hereinafter *Cal. Search Warrant Case*].

164. *N.Y. Search Warrant Case*, at *6.

165. *Id.* at *1.

166. *Cal. Search Warrant Case*, at *1.

167. Benner & Lichtblau, *supra* note 143.

168. APPLE, *supra* note 16.

169. *Id.*

It is clear that Apple prioritizes data security and privacy by limiting the dissemination of information that it has collected.[170] However, its privacy practices have been criticized as lackluster for the collection of personal information that it believes necessary to improve its products.[171] Jeffrey Paul, a security blogger, pointed out that Apple's new operating system automatically uploads unsaved copies of many programs to iCloud in order to ensure that a user can pick up from where she left off.[172] Since documents released by Edward Snowden about the National Security Agency's PRISM program listed Apple as "involved," any information sent to iCloud could become a part of a federal data-mining program.[173] However, Apple states that it was never subject to any orders for bulk data by the NSA,[174] and it seems unlikely Apple actually participated in the PRISM program.[175]

Apple has taken some steps to protect a self-declared user's right to privacy. They have, for example, built encryption into their texting service, iMessage, and calling service, FaceTime.[176] It appears that on the whole Apple's commitment to privacy is among the strongest for service providers. One journalist pointed out that is likely because its advertising system failed, and Apple does not reap the same benefits from selling user data as its competitors and therefore has made this choice out of business necessity.[177]

---

170. *See Privacy Built in*, APPLE, https://www.apple.com/privacy/privacy-built-in/ (last visited Mar. 29, 2015) (describing the situations in which a customer's data is, or is not, disseminated).

171. Thorin Klosowski, *Let's Talk About Apple's Privacy Issues*, LIFEHACKER (Nov. 10, 2014, 4:00 AM), http://lifehacker.com/lets-talk-about-apples-privacy-issues-1655944758.

172. Jeffrey Paul, *iCloud Uploads Local Data Outside of iCloud Drive*, DATAVIBE (Oct. 23, 2014), https://datavibe.net/~sneak/20141023/wtf-icloud/.

173. "The top-secret PRISM program allows the U.S. intelligence community to gain access from nine Internet companies to a wide range of digital information, including e-mails and stored data, on foreign targets operating outside the United States." *NSA Slides Explain the PRISM Data-Collection Program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

174. *See* APPLE, *supra* note 16.

175. *Apple's Commitment to Customer Privacy*, APPLE (June 16, 2013), https://www.apple.com/apples-commitment-to-customer-privacy/ ("We do not provide any government agency with direct access to our servers, and any government agency requesting customer content must get a court order.")

176. *Privacy Built in*, *supra* note 170.

177. David Goldman, *Tim Cook Didn't Address Apple's Real Privacy Problem*, CNNMONEY (Sept. 8, 2014, 4:45 PM), http://money.cnn.com/2014/09/18/technology/security/apple-privacy/.

The final question is whether Apple could be considered a state actor. It would be fairly hard to characterize Apple as either entwined with government or performing traditional governmental functions. The strongest argument likely depends on the relationship between Apple and law enforcement agencies. That argument would start by examining whether Apple has been directed by government to include certain front-door access on their devices to allow government agents to search a user's phone. However, this is unlikely to be near the level of *Marsh v. Alabama*,[178] and therefore, it is very unlikely that a court would find Apple to be a government actor.

B. Google

Google was founded in 1998 as a company that sought to organize the Internet through a better search product.[179] It has been wildly successful and continues to dominate the search market in the United States with a 64.5% share of all desktop search queries.[180] It has also moved into e-mail, social networking, video, maps, browsers and cell phones among many, many other products.[181] It has truly transformed the accessibility of information and continues to innovate in fascinating and breathtaking ways.[182] It has sought to accomplish all this while staying true to its founding mission.[183]

As Google makes almost all of its money off advertising,[184] it has sought to ensure that advertisers are actually reaching their

178. *See Marsh*, 326 U.S. at 507–08.

179. *Our History in Depth*, GOOGLE, http://www.google.com/about/company/history/ (last visited Apr. 3, 2015).

180. *comScore Explicit Core Search Share Report*, COMSCORE (Mar. 17, 2015), http://www.comscore.com/Insights/Market-Rankings/comScore-Releases-February-2015-US-Desktop-Search-Engine-Rankings.

181. *Products*, GOOGLE, https://www.google.com/intl/en/about/products/ (last visited Sept. 26, 2016).

182. *Self-Driving Car Test: Steve Mahan*, GOOGLE, http://www.google.com/about/careers/lifeatgoogle/self-driving-car-test-steve-mahan.html (last visited Apr. 3, 2015).

183. Google seeks to focus on a list of ten items including "[f]ocus on the user and all else will follow," and "[i]t's best to do one thing really, really well." *What We Believe*, GOOGLE, http://www.google.com/about/company/philosophy/ (last visited Apr. 3, 2015).

184. In its most recent filing, Google made roughly 90% of its revenue from advertising. *2014 Financial Tables*, GOOGLE, https://investor.google.com/financial/tables.html (last visited Apr. 3, 2015).

targeted audience through the use of big data analytics.[185] Google also seeks to perfect its search algorithm to further capture a larger section of the U.S. desktop search market.[186] In addition, they seek to retain their power as more consumers use mobile devices to access Google's search engine.[187]

Google is able to introduce all these new web services because by gathering data through the provisioning of services, it is building an enormous database of information on each of its users. Through this database, it has a fairly comprehensive view of the likes, dislikes, interests and disinterests of each of its users. Google then sells this highly sought after information to advertisers who wish to reach a certain type of individual through its Adwords program.[188]

Google recognizes that individuals must be willing to part with this information, and they therefore recognize the importance of their users.[189] According to their guiding philosophy, they seek to "focus on the user and all else will follow."[190] As Google is a leader in search and e-mail, it is the recipient of many governmental requests.[191] In the period from January 1 to June 30, 2014, Google received over 12,539 requests from governments in the United States and provided information 84% of the time.[192] Google says that it does "often successfully" challenge facially broad or problematic legal processes.[193]

In addition, there are several cases in which Google has challenged legal processes in court.[194] Like many of the challenges to

185. Neil Mohan, *Toward Viewability: You Can't Count What You Haven't Measured*, THINK NEWSLETTER (Mar. 2015), https://www.thinkwithgoogle.com/articles/toward-viewability-advertising-measurement.html.

186. James Martin, *How To Prepare for Google's Next Major Search Update*, CIO (Apr. 2, 2015, 4:42 AM), http://www.cio.com/article/2905192/seo-sem/how-to-prepare-for-googles-next-major-search-update.html.

187. *Id.*

188. *See Adwords*, GOOGLE, https://www.google.com/adwords/ (last visited Apr. 18, 2015).

189. *See What We Believe*, *supra* note 183.

190. *Id.*

191. *See Transparency Report: Countries Table*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/countries/?t=table (last visited Apr. 18, 2015).

192. *Id.*

193. *Transparency Report: Legal Process*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/legalprocess (last visited Apr. 18, 2015).

194. *See, e.g.*, Gonzales v. Google, Inc., 234 F.R.D. at 678 (challenging the Department of Justice's use of the Child Online Protection Act to subpoena information about Google search queries); Karen Gullo, *Google Fights U.S. National Security Probe Data Demand*, BLOOMBERG LAW (Apr. 4, 2013, 12:01 AM), http://www.bloomberg.com/news/articles/2013-04-04/google-fights-u-s-national-security-probe-data-

legal process it is unclear if Google's purpose was the protection of their users' privacy or other business reasons. The case that Google itself points to on its website is *Gonzales v. Google* from 2006.[195] In that case, Google challenged a Department of Justice subpoena for search records for use in a separate case challenging the constitutionality of the Child Online Protection Act (COPA).[196] While the Department of Justice subpoenaed many companies, the only company to challenge the subpoena was Google.[197]

Some commentators at the time pointed out that Google did not mention privacy in their arguments, but that this case was truly about protecting their business practices.[198] At the time, many did not take seriously the argument that strings of search terms could not reveal private details.[199] However, as the enterprising work of Arvind Narayanan and Vitaly Shmatikov showed in their paper about the Netflix Prize several years later, almost any dataset can be used to discover private information about the users.[200] Google relied on a theory about protecting its trade secrets from preventing this information from being released.[201] In the court's decision, it found that users had some expectation of privacy in their search results, notwithstanding Google's privacy policy,[202] and that Google had a legitimate interest in protecting its trade secrets.[203] In the end, Google was forced to give the government 50,000 randomly selected URLs that Google had catalogued for purposes of its search.[204]

Since this case in 2006, from publicly available documents it is not clear if Google has challenged other subpoenas or warrants in court. On the other hand, they have challenged National Security Letters that they have received.[205] Unfortunately, most of the court

---

demand (discussing Google's challenge to the National Security Letters, but the challenge is under seal).

195. *See Transparency Report: Legal Process*, *supra* note 191.

196. *Gonzales*, 234 F.R.D. at 678.

197. *E.g.* Adam Liptak, *In Case About Google's Secrets, Yours Are Safe*, N.Y. TIMES (Jan. 26, 2006), http://www.nytimes.com/2006/01/26/technology/26privacy.html?pagewanted=all.

198. *Id.*

199. *Id.*

200. Arvind Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets*, *in* 2008 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 111, 121–23 (2008).

201. Liptak, *supra* note 197.

202. *Gonzales*, 234 F.R.D. at 684.

203. *Id.* at 685.

204. *Id.* at 681–82, 688.

205. *See* Gullo, *supra* note 194.

documents are under seal pursuant to 18 U.S.C. § 2709, which prohibits disclosure of the legal process.[206]

Google has spent quite a bit of time and money on defending their user base from overbroad legal process, but they also likely have as much if not more data than most other companies out there. As the recent European Union antitrust Statement of Objections makes clear, Google has the ability to, and often does, prioritize search results favoring certain internal companies.[207] Unfortunately, because Google still seeks to protect its search algorithm, it is not clear how often they direct searches to internal websites. In addition, Google has the ability to favor certain products, but justifies this change on the basis of attempting to improve search results.[208] It is unlikely that Google currently changes search results to favor a particular class or party, but it is likely that they already change search results to favor certain products. Finally, Google examines the content of its users' e-mail for purposes of providing advertising related to that content.[209] In doing so, Google claims that their users' e-mails do not have a reasonable expectation of privacy.[210]

Google does not fit within any of the exceptions to the state actor problem. Search engines are not something that was required before the advent of the Internet. Government never had the opportunity to turn search into a traditional governmental function. Therefore, even though Google controls the ecosystem in which millions spend their days, they provide products for which government has very rarely offered. It is unlikely that a judge would find Google to be a state actor.

C. Microsoft

Microsoft is one of the oldest Internet companies in the world. Bill Gates and Paul Allen founded it in 1975 to focus on personal

206. 18 U.S.C. § 2709(c)(1)(A) (2012).

207. Fact Sheet, European Commission, Antitrust: Commission Sends Statement of Objections to Google on Comparison Shopping Service (Apr. 15, 2015), http://europa.eu/rapid/press-release_MEMO-15-4781_en.htm.

208. Brody Mullins, Rolfe Winkler & Brent Kendall, *Inside the U.S. Antitrust Probe of Google*, WALL ST. J. (Mar. 19, 2015, 7:38 PM), http://www.wsj.com/articles/inside-the-u-s-antitrust-probe-of-google-1426793274.

209. Samuel Gibbs, *Gmail Does Scan All Emails, New Google Terms Clarify*, GUARDIAN (Apr. 15, 2014, 8:24 AM), http://www.theguardian.com/technology/2014/apr/15/gmail-scans-all-emails-new-google-terms-clarify.

210. *Id.*

computing.[211] According to NetMarketShare, a company that determines the market share of various Internet companies, in March 2015 Microsoft's Windows operating system had a roughly 91% share of the desktop market.[212] Microsoft has also expanded into other product lines including video games, search, mobile phones, e-mail, cloud storage, office tools, and web browsing.[213] Each of these products has the ability to create a tremendous amount of data, and Microsoft is often seen as a direct competitor to Google.

Microsoft has a cross-interface ID that is often required to sign into many of its services.[214] This allows Microsoft to follow its users from the games they play on their Xbox system to their e-mails and even their word documents.[215] Microsoft, after years of catch up to Google, has created a multiplatform ecosystem that people use for work and leisure. In pursuit of Google, Microsoft has sought to identify itself as the company that takes privacy more seriously than Google or other competitors.[216] For instance, in a white paper on the topic of trust in its Office product, which includes Microsoft Word, Excel, and Outlook, Microsoft seeks to distinguish itself from the competing Google product on privacy.[217] Microsoft claims that its products are more secure and its terms are more straightforward on how it seeks to use data from these Office products.[218]

Microsoft also has a historical reason to be more protective of privacy. For years, Microsoft's Windows has been the dominant op-

211. *A History of Windows*, MICROSOFT, http://windows.microsoft.com/en-us/windows/history#T1=era0 (last visited Apr. 19, 2015).

212. Desktop Operating System Market Share, NETMARKETSHARE, http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0 (last visited Apr. 19, 2015) (added the market share of Windows 10 (0.09%), 8.1 (10.55%), 8 (3.52%), 7 (58.04%), Vista (1.97%), XP (16.94%), NT (0.08%), 2000 (0.01%) & 64 (0.01%)).

213. *13 Most Important Microsoft Product Lines*, REDMOND MAGAZINE (Jan. 3, 2012), http://redmondmag.com/articles/2012/01/01/13-most-important-microsoft-product-lines.aspx.

214. *What is Microsoft ID*, MICROSOFT, http://windows.microsoft.com/en-us/windows-live/sign-in-what-is-microsoft-account (last visited Apr. 19, 2015) ("Your Microsoft account is the combination of an email address and a password that you use to sign in to services like Outlook.com, OneDrive, Windows Phone, or Xbox LIVE.")

215. *Id.*

216. *See Trust in Office 365*, MICROSOFT, http://www.whymicrosoft.com/see-why/trust-office-365/ (last visited Apr. 19, 2015) (identifying the various ways that Microsoft integrated privacy protections into their products, while noting that "Google has been embroiled in lawsuits arising from questionable usage of user data").

217. *Id.*

218. *Id.*

erating system,[219] and its Office suite has been the dominant productivity tool used in homes and offices around the world.[220] Unfortunately Microsoft does not break out its revenue from Bing as compared to the rest of its online software.[221] This has allowed Microsoft, by nature of its business model, to view search as a short-term money loser, but important long-term asset for keeping people in the Microsoft ecosystem.[222] In other words, Microsoft does not rely entirely on revenue from ad sales and therefore is able to use its revenue from its consumer and business hardware and software divisions to effectively subsidize its stronger privacy settings.

As part of this commitment to privacy, Microsoft's transparency report shows that it rejects over 16% of the U.S. governments' requests for information and does not find data in an additional 15% of requests.[223] Therefore, it only hands over information in 69% of requests.[224]

On the other hand, Microsoft recently was caught looking through a user's e-mail contents as part of an investigation into internal leaks.[225] In the aftermath of this revelation, Microsoft committed itself to a series of standards, which could and should provide a model for companies looking to scan the contents of an e-mail by one of their users.[226]

---

219. *See* Desktop Operating System Market Share, *supra* note 210.

220. *See* Trefis Team, *Microsoft Earnings Preview: Hardware and Cloud Sales in Focus*, FORBES (Jan. 22, 2015, 2:17 PM), http://www.forbes.com/sites/greatspeculations/2015/01/22/microsoft-earnings-preview-hardware-and-cloud-sales-in-focus/ ("Currently, we estimate that the company has close to 93% share in productivity software market.").

221. *Earnings Release FY15 Q2: Devices & Consumers Other*, MICROSOFT, http://www.microsoft.com/Investor/EarningsAndFinancials/Earnings/SegmentResults/S3/FY15/Q2/Performance.aspx (last visited Apr. 20, 2015).

222. Alex Wilhelm, *Microsoft's Long, Winding Road to Online Profits and a Break-Even Bing*, THE NEXT WEB (Jan. 13, 2013), http://thenextweb.com/insider/2013/01/25/microsoft-5/.

223. *Law Enforcement Requests Report: 2014 (Jul-Dec): United States*, MICROSOFT, http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/ (last visited Apr. 20, 2015).

224. *Id.*

225. Russell Brandom, *Microsoft Just Exposed Email's Ugliest Secret,* VERGE (Mar. 12, 2014, 2:10 PM), http://www.theverge.com/2014/3/21/5533814/google-yahoo-apple-all-share-microsofts-troubling-email-privacy-policy.

226. *See* Microsoft Corporate Blogs, *Strengthening Our Policies for Investigations*, MICROSOFT (Mar. 20, 2014), http://blogs.microsoft.com/on-the-issues/2014/03/20/strengthening-our-policies-for-investigations/.

> [1] [Microsoft] will not conduct a search of customer e-mail and other services unless the circumstances would justify a court order, if one were available.
>
> [2] . . . [Microsoft] will rely in the first instance on a legal team separate from the internal investigating team to assess the evidence. We will move forward only if that team concludes there is evidence of a crime that would be sufficient to justify a court order, if one were applicable. . . . [W]e will then submit this evidence to an outside attorney who is a former federal judge. We will conduct such a search only if this former judge similarly concludes that there is evidence sufficient for a court order.
>
> [3] . . . [A search will] be confined to the matter under investigation and not search for other information. . . .
>
> [4] . . . We therefore will publish as part of our bi-annual transparency report the data on the number of these searches that have been conducted and the number of customer accounts that have been affected.[227]

The Microsoft standards fulfill many of the same requirements placed on law enforcement. First, because Microsoft raises the standard by which its own employees can search through the contents of an e-mail account.[228] Second, it provides limited due process by which an independent party evaluates the evidence to ensure it meets a minimum standard.[229] Third, there is a particularity requirement—confining the search to the matter under investigation—that protects against unwarranted fishing expeditions into the user's data.[230] Finally, Microsoft will publish the information.[231] Unfortunately, in these requirements Microsoft does not include any information about notifying the user of the search, nor do they allow the user to challenge the invasion prior to the search. Other companies such as Apple, Google, and Yahoo agree with Microsoft that they have the right to search users' e-mails but only Microsoft provides an overview of its internal procedures to look at the information.[232]

---

227. *Id.*

228. *Id.*

229. *Id.*

230. *Id.*

231. *Id.*

232. Alex Hern, *Yahoo, Google and Apple Also Claim Right To Read User Emails*, GUARDIAN (Mar. 21, 2014, 1:08 PM), http://www.theguardian.com/technology/2014/mar/21/yahoo-google-and-apple-claim-right-to-read-user-emails.

This is an important step forward in protecting against internal pressures to seek the content of information. Microsoft has also held the government to similar standards by protecting its users from unlawful or facially deficient legal processes.[233] In the recent *In re Warrant*, Microsoft sought to quash a court order issued by a Magistrate Judge for the contents of an e-mail account in Ireland.[234] While the Magistrate, affirmed by the district court, held that the court order was a hybrid warrant and subpoena allowing for jurisdiction over the user's account in Ireland,[235] Microsoft has sought to defend the privacy of its user under a number of theories.

Microsoft's arguments stemmed around the collateral effects of the United States asserting jurisdiction over data held on a server in another country. As Microsoft wrote, the case comes down to whether the location of the "'execution of a search warrant' to retrieve communications from 'electronic storage,'" is relevant to the question of jurisdiction.[236] Microsoft has often repeated that it is seeking to protect the privacy of its users, but it is also clear Microsoft has business reasons in arguing in favor of this case.[237] Microsoft has a robust European business, and European leaders have begun to question U.S. data privacy laws.[238] This is important since there is currently a debate about whether the Safe Harbor agreement between the United States and the E.U. should be revised.[239] This agreement allows for the cross continent sharing of data and allows Microsoft and other multinational companies to operate in both Europe and the United States and allow for data to be transferred freely back and forth between companies in the two continents.[240]

Microsoft has become a leader in privacy protection by seeking to place internal controls on its staff and fighting against unlawful

233. *E.g. In re* Warrant To Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y.), *aff'd*, No. 13-MJ-2814, 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014) [hereinafter *In re Warrant*].

234. *Id.* at 467.

235. *Id.* at 471.

236. Reply Brief for Appellant at 6, Microsoft Corp. v. United States, No. 14-2985 (2d Cir. Apr. 8, 2015), 2015 WL 1754413, at *5 (quoting 18 U.S.C. 2703(a), (g)).

237. Microsoft Corporate Blogs, *Business, Media and Civil Society Speak Up in Key Privacy Case*, MICROSOFT (Dec. 15, 2014), http://blogs.microsoft.com/blog/2014/12/15/business-media-civil-society-speak-key-privacy-case/.

238. Sam Schechner & Valentina Pop, *Personal Data Gets Day in Court*, WALL ST. J. (Mar. 24, 2015, 3:58 PM), http://www.wsj.com/articles/court-hears-challenge-to-safe-harbor-data-deal-1427206554.

239. *Id.*

240. *Id.*

government invasion. It can continue these strong efforts as it further competes with Google in search. While it competes with Google in many areas, it shares with Google the fact that a court is unlikely to find it to be a state actor. Microsoft does not perform a traditional state function nor does it appear to be so entwined with government. However, just like Google, on first principles, people spend their entire day within Microsoft's ecosystem. In addition, Microsoft's products are indispensable to business executives seeking to participate in modern commerce. This still is not likely enough to make the case that Microsoft should be considered a state actor.

D. Facebook

Facebook, famously founded in a dorm room in 2004, is an enormous social media platform.[241] It also controls the market for social logins in which people use Facebook in order to log into other nonaffiliated websites.[242] Facebook's main business is ad sales on its website, its mobile site, and on other web and mobile sites.[243] One of the benefits of Facebook is that it has access to thousands of data points on individuals and with this data can accurately predict many different things including personality traits.[244] A recent study showed that "computer' judgments of people's personalities based on their digital footprints are more accurate and valid than judgments made by their close friends or acquaintances."[245]

Facebook recently changed its policy to tracks users across the web to provide a more targeted advertising experience.[246] According to the executive in charge of advertising for Facebook, people

241. Sarah Phillips, *A Brief History of Facebook*, GUARDIAN (July 25, 2007, 5:29 PM), http://www.theguardian.com/technology/2007/jul/25/media.newmedia.

242. Frederic Lardinois, *Facebook Continues To Dominate Social Logins, Expands Lead to 61% Market Share*, TECHCRUNCH (Jan. 27, 2015), http://techcrunch.com/2015/01/27/facebook-dominates-social-logins/.

243. *What Are Facebook's Main Revenue Streams?*, YAHOO (May 25, 2006), http://finance.yahoo.com/news/facebook-main-revenue-streams-130759705.html.

244. *See* Wu Youyou et al., *Computer-Based Personality Judgments Are More Accurate than Those Made by Humans*, 112 PROC. NAT'L ACAD. SCI. 1036, 1039 (2015) (stating that computer-based models are able to accurately judge people's personalities).

245. *Id.* at 1036.

246. Violet Blue, *Facebook Turns User Tracking 'Bug' into Data Mining 'Feature' for Advertisers*, ZDNET (June 17, 2014, 12:01 AM), http://www.zdnet.com/article/facebook-turns-user-tracking-bug-into-data-mining-feature-for-advertisers/.

specifically requested a more targeted advertising environment.[247] From the quotation, it is unclear whether he is referring to advertisers or users of Facebook. This is actually a much larger problem for companies to define their constituents.[248] For many companies such as Facebook that make all of their money through advertising, users are part of the product itself.[249]

Facebook has acknowledged that it has vast amounts of data within its control.[250] Through the use of this data, Facebook has customized a user's experience, including by deciding what information to display on their Facebook wall.[251] Facebook has complete control of content that its users see and has even made some users wary of their relationship with certain individuals because they did not see any Facebook news stories.[252] In addition, many individuals in a study reported that they believed it was their fault if they missed an important news event about their friend, rather than the algorithm failing to post the story.[253]

One of Facebook's main missions is to provide users with the power to share information about their lives to family and friends.[254] In order to do this, users must sacrifice some privacy to provide any interesting information or photographs about their life. Facebook would have to change its business model if its users stopped supplying information to Facebook. It also recognizes that it must be a responsible guardian of that data. While Facebook receives many government data requests, they only produce data 79% of the time, including 72% for subpoenas and 84% for warrants.[255]

247. Vindu Goel, *Facebook To Let Users Alter Their Ad Profiles*, N.Y. TIMES (June 12, 2014), http://www.nytimes.com/2014/06/13/technology/facebook-to-let-users-alter-their-ad-profiles.html?_r=0.

248. *See, e.g.*, Olivia Solon, *You Are Facebook's Product, Not Customer*, WIRED (Sept. 21, 2011), http://www.wired.co.uk/news/archive/2011-09/21/doug-rushkoff-hello-etsy (explaining that often the interests of the people who pay for a product, advertisers, and the people who use a product, users, often do not align).

249. *Id.*

250. *Research at Facebook*, FACEBOOK, https://research.facebook.com/datascience (last visited Apr. 3, 2015).

251. Motahhare Eslami et. al., *"I Always Assumed that I Wasn't Really that Close to [her]": Reasoning About Invisible Algorithms in the News Feed*, HUM. FACTORS IN COMPUTING SYS. CONF. (2015), http://social.cs.uiuc.edu/papers/pdfs/Eslami_Algorithms_CHI15.pdf.

252. *Id.* at 6.

253. *Id.* at 4.

254. *Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/ (last visited Apr. 3, 2015).

255. *Government Request Reports: United States: July 2014–December 2014*, FACEBOOK, https://govtrequests.facebook.com/country/United%20States/2014-H2/ (last visited Apr. 3, 2015).

They have also gone to court to defend their users against government requests.[256]

In one recent case currently on appeal, the New York County District Attorney requested, pursuant to a validly issued search warrant, "virtually all communications, data, and information from 381 Facebook accounts, yet only 62 of the targeted Facebook users were charged with any crime."[257] Facebook is fighting against this overbroad request by arguing, among other reasons, that it "has third-party standing to assert the constitutional rights of its users whose private information has been seized without notice and is being held by the Government."[258] In addition, it sought to argue that since the warrant is broad and lacking particularity, it should not have to execute the warrant.[259] Facebook does not specifically assert or state a broad right to privacy found in the Fourth Amendment, but instead simply refers to the violation of constitutional rights of its users because their information would be seized and they would have no knowledge.[260]

In another case, Facebook sought to challenge a civil subpoena because it believed that the subpoena did not fall within the narrow exceptions under the Stored Communications Act.[261] Once again it did not state that it was protecting its user's (a deceased woman from England) privacy, but rather that under the statute, service providers have no obligation to provide the information.[262] One possible reason that Facebook fought against this subpoena is that it did not want to become deluged by civil subpoenas. Instead, through civil discovery, much of this information can and must be produced pursuant to civil procedure.[263]

---

256. *See generally In re* Facebook, Inc., 923 F. Supp. 2d 1204, 1205–06 (N.D. Cal. 2012) (holding that civil subpoena violated the Stored Communications Act); Brief for Facebook at 1, *In re* 381 Search Warrants Directed to Facebook Inc., 14 N.Y.S.3d 23 (App. Div. 2015), No. 30207-13 [hereinafter *Brief for Facebook*] (appealing dismissal of Facebook's motion to quash warrants for Facebook user accounts).

257. *Brief for Facebook*, supra note 256, at 3.

258. *Id.* at 7.

259. *Id.*

260. *Id.* at 24–25.

261. Facebook's Motion To Quash Subpoena at 5, *In re* Facebook, Inc., 923 F. Supp. 2d 1204 (N.D. Cal. 2012) (No. 5:12-mc-80171-LHK), 2012 WL 8505651.

262. *Id.*

263. Jason Lien & Jesse Mondry, *Litigation: When Discovery of Social Media Makes Sense in Civil Cases*, INSIDE COUNSEL (Aug. 15, 2013), http://www.insidecounsel.com/2013/08/15/litigation-when-discovery-of-social-media-makes-se.

Facebook has faced many criticisms for its internal privacy policy.[264] Facebook has a comprehensive website outlining its policies, but it is even apparent from its privacy website that Facebook allows its own internal personnel, third parties, or advertisers to look at sensitive user data unrestricted.[265]

Finally, Facebook is the new public forum in which people discuss the day's events, share news, and sometimes debate controversial topics. At the founding of the country, it is likely that these events all occurred on the street corner or in the parks. Government sought to protect those places and continues to respect and protect constitutional rights in public forum. Therefore, Facebook is the town in *Marsh v. Alabama*. Only it appears to be a virtual town, and Facebook has essentially created a government over that virtual town. A strong case could be made that Facebook should be considered a state actor since it has encroached on a traditional governmental function of protecting public spaces.

E. Amazon

Amazon is a global e-commerce site founded in 1995.[266] According to its mission statement, "[Amazon] seek[s] to be Earth's most customer-centric company for four primary customer sets: consumers, sellers, enterprises, and content creators."[267] According to data from 2013, Amazon has more revenue from e-commerce in the United States than the next nine sites combined.[268] In addition, Amazon has taken dominant positions in the e-book market.[269] Finally, Amazon's cloud computing service has a dominant 30% mar-

264. *See generally* Sam Schechner, *Facebook Privacy Controls Face Scrutiny in Europe,* WALL ST. J. (Apr. 2, 2015), http://www.wsj.com/articles/facebook-confronts-european-probes-1427975994 (describing how several European regulators initiated investigations into Facebook's privacy controls).

265. *Data Policy*, *supra* note 254.

266. *FAQs*, AMAZON, http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-faq (last visited Mar. 25, 2015).

267. Kimberly B., *People and Purpose: What Amazon's Jeff Bezos Teaches Us About Values*, IMS BLOG (July 1, 2014), http://www.ims.gs/blog/people-purpose-amazons-jeff-bezos-teaches-us-values/.

268. Amazon made $67.86 billion in 2013 in online sales, while the next nine companies made $64.61 billion. Internet Retailer, *Leading E-retailers in the United States in 2013, Ranked by E-commerce Sales (in Billion U.S. Dollars)*, STATISTA, http://www.statista.com/statistics/293089/leading-e-retailers-ranked-by-annual-web-e-commerce-sales/ (last visited Mar. 25, 2015).

269. Digitimes, *Market Share of Amazon's Kindle E-readers from 2008 to 2011*, STATISTA, http://www.statista.com/statistics/276508/global-market-share-of-amazons-kindle-e-readers/ (last visited Mar. 25, 2015) (stating that in 2010 Amazon accounted for 62.8% of all e-reader shipments).

ket share worldwide.[270] It is no exaggeration to say that Amazon plays an enormous role in the daily life of millions of Americans. It also collects information about a consumer's purchasing history from among its many internal websites and other affiliates.[271] This data can be used for any number of tasks. Therefore, Amazon has the ability to examine the purchasing habits, reading habits, e-mail, blog posts, and photographs among other items of millions of its users. Yet Amazon alone among major technology companies seems to be dragging its feet on privacy. For instance, it has failed to join its competitors in the industry in releasing a transparency report about the number of data requests it receives from governments around the world.[272]

While Amazon's transparency clearly compares negatively to its competitors' transparency, it has fought against the U.S. government on behalf of its users.[273] It has mainly relied on First Amendment grounds to challenge the government's request for information about its customers by arguing that the "buying and selling of expressive materials are protected activities under the First Amendment."[274] In a brief in a case against North Carolina, Amazon lists several books that they believe could cause harm to the purchaser if their existence was released to the government, including *He Had It Coming: How to Outsmart Your Husband and Win Your Divorce* and *Outing Yourself: How to Come Out as Lesbian or Gay to Your Family, Friends, and Coworkers*.[275]

There is an alternative explanation for why Amazon fights for its users' privacy and it involves one of the two certainties in life—

270. AWS Market Share Reaches Five-Year High Despite Microsoft Growth Surge, SYNERGY RESEARCH GROUP (Feb. 2, 2015), https://www.srgresearch.com/articles/aws-market-share-reaches-five-year-high-despite-microsoft-growth-surge.

271. *See Amazon.com Privacy Notice*, AMAZON (Mar. 3, 2014), https://www.amazon.com/gp/help/customer/display.html?nodeId=468496.

272. Zach Whittaker, *Amazon Doesn't Want You to Know How Many Data Demands It Gets*, ZDNET (Mar. 19, 2015, 7:34 AM), http://www.zdnet.com/article/amazon-dot-com-the-tech-master-of-secrecy/.

273. *See, e.g.*, Amazon.com LLC v. Lay, 758 F. Supp. 2d 1154, 1171–72 (W.D. Wash. 2010) (granting summary judgment for Amazon against the Secretary of North Carolina Department of Taxation for the Secretary's invalid request for the names of customers on Amazon.com); *In re* Grand Jury Subpoena to Amazon.com Dated Aug. 7, 2006, 246 F.R.D. 570, 576 (W.D. Wis. 2007) (unsealing court order regarding Amazon's successful motion to quash grand jury subpoena of personal identifying information for certain customers).

274. Amazon's Motion for Summary Judgment at 8, Amazon.com LLC v. Lay, 758 F. Supp. 2d 1154 (W.D. Wash. 2010) (No. 10-CV-00664), ECF No. 44 [hereinafter *Brief for Amazon*].

275. *Id.* at 6.

taxes. For a long time, Amazon fought against forcing its users to pay sales tax because without sales tax, it can charge less for shopping online.[276] This is likely why Amazon challenged the Department of Taxation in North Carolina when it tried to subpoena the names and addresses of North Carolina customers of Amazon.[277]

Amazon's arguments, while self-serving, create a viable framework for challenging a government subpoena of certain transactional records, especially book and movie purchases. The larger question is how does Amazon protect those same First Amendment rights against which it is afraid of government intrusion. Justice Marshall in *Stanley v. Georgia* wrote that "[i]f the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch."[278] In Amazon's own briefs, it cites approvingly to Justice Marshall's *Stanley* opinion.[279] In addition, it argues that "[a]nonymity is a shield from the tyranny of the majority."[280]

Since Amazon collects data that would allow the company to recommend certain new products and seems to know who is purchasing certain books and films, Amazon's statement that it is protecting the First Amendment rights of its customers seems to ring hollow. While the First Amendment does not bind Amazon, a private corporation,[281] Amazon has the capability to pierce the anonymity that was once a given when someone purchased a book at a local bookstore. Today, a user's Amazon purchase history can provide extremely valuable insight into the mindset of that consumer.[282] For instance, Amazon can use this information to promote a particular product and, by analyzing its data, can determine the best customers to whom to recommend that product.[283] If Amazon knows what a customer owns, and can predict with a high degree of certainty a product that the customer will enjoy, the cus-

276. Alexia Elejalde-Ruiz & Gregory Karp, *Amazon To Start Collecting Illinois Sales Tax*, CHI. TRIB. (Jan. 23, 2015, 7:32 PM), http://www.chicagotribune.com/business/breaking/ct-amazon-sales-tax-illinois-0124-biz-2-20150123-story.html ("Amazon sales are likely to decline about 10 percent in Illinois if its pattern follows those of other states, according to Itzhak Ben-David.").

277. *See* Stan Chambers Jr., *Amazon To Collect NC Sales Tax*, WRAL (Jan. 18, 2014), http://www.wral.com/Amazon_to_collect_NC_sales_tax/13310401/.

278. Stanley v. Georgia, 394 U.S. 557, 565 (1969).

279. *See Brief for Amazon*, *supra* note 272, at 8.

280. *Id.* at 9 (*citing* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995)).

281. *See* discussion on State Actor Doctrine, *supra* Part II.

282. JP Mangalindan, *Amazon's Recommendation Secret*, FORTUNE (July, 30, 2012, 11:09 AM), http://fortune.com/2012/07/30/amazons-recommendation-secret/.

283. *Id.*

tomer is left at the mercy of the product-recommendation algorithm. Amazon can also seek to tailor the price to the consumer by engaging in price discrimination.[284] One company claims that by giving a discount to the group of individuals that is most likely to leave the website, they could increase revenue five percent.[285]

Does Amazon, standing as a private company, seek to tell its users what books they should buy? It would appear that their algorithm has the capability to at the very least suggest, if not "prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion."[286] Amazon would clearly claim that their algorithm is narrowly tailored to further its interest in selling more books to its users and making a profit. Amazon is, after all, a company that seeks to increase its profit above all else.[287] In addition, if users feel that they are being discriminated against, they can move their business to another website such as Google. According to the former Google Chief Executive Officer Eric Schmidt, Google sees Amazon as its primary competitor since Amazon has essentially become a search engine for shopping.[288]

Finally, Amazon likely would not be considered a state actor. The Supreme Court has continuously found that private shopping centers are not state actors.[289] Therefore, analogizing Amazon to a private shopping center would make Amazon likely not a state actor. However, a traditional government role has been the provision of public libraries. Amazon has begun to replace the public library with a system of sharing. Under the public function doctrine, Amazon would have to completely usurp the role of government. It does

284. *See* Adam Tanner, *Different Customers, Different Prices, Thanks To Big Data*, FORBES (Mar. 26, 2014, 6:00 AM), http://www.forbes.com/sites/adamtanner/2014/03/26/different-customers-different-prices-thanks-to-big-data/.

285. *See id.* This company, Freshplum, was acquired by TellApart, which claims that it "brings a data-modeled approach to offers that ensures each promotion is presented to just the shopper who needs it to drive a purchase." *Solutions,* TELLAPART, http://www.tellapart.com/solutions/#audience-targeting (last visited Apr. 17, 2015).

286. W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 642 (1943).

287. Friedman, *supra* note 42.

288. Jeevan Vasagar & Alex Barker, *Amazon Is Our Biggest Search Rival, Says Google's Eric Schmidt*, FIN. TIMES (Oct. 13, 2014), http://www.ft.com/intl/cms/s/0/748bff70-52f2-11e4-b917-00144feab7de.html#axzz3G2xWwdei ("In search, he said that 'many people think our main competition is Bing or Yahoo. But, really, our biggest search competitor is Amazon', pointing out that Internet users are likely to go directly to the retailer if they are shopping.").

289. *See, e.g.*, Lloyd Corp. v. Tanner, 407 U.S. 551, 570 (1972) (holding that a private shopping center was not a state actor and therefore the plaintiff could not assert a First Amendment right).

not appear that Amazon is doing so, and private libraries can and do exist. In addition, private universities often are not considered state actors even though they have libraries and often perform other traditional roles of government.[290]

F. Comcast

Comcast, founded in 1963, was an early cable television system in Tupelo, Mississippi.[291] Through acquisitions and investments, Comcast has come to dominate the cable industry, the broadband industry, and after its purchase of NBCUniversal, the entertainment industry. For example, it currently provides over half of the broadband access, as recently defined by the FCC, in the United States.[292] Through this dominance, Comcast controls both the content that people want to see on sites like Hulu and NBC and the physical infrastructure for users to get online.

Comcast currently collects certain metadata information from its customers.[293] Comcast can use this metadata, such as IP addresses and port numbers for websites, to keep track of web-browsing history[294] and also create a log of television-viewing habits.[295]

Comcast, unfortunately, does not have any statements or public legal documents framing its internal conversation on privacy responses to the federal government. While there is a case in the public record, the records from that case are too old to be found online.[296] It is regulated more heavily than many other companies on the EFF's list because it falls under two federal laws regulating

290. *See, e.g.*, Reichert v. Elizabethtown Coll., No. 10-2248, 2011 WL 3438318, at *3 (E.D. Pa. Aug. 5, 2011) (holding that the state does not exercise sufficient control over the college).

291. *Timeline*, COMCAST, http://corporate.comcast.com/news-information/timeline (last visited Mar. 29, 2015).

292. Jon Brodkin, *Comcast Now Has More than Half of All US Broadband Customers*, ARS TECHNICA (Jan. 30, 2015, 10:34 AM), http://arstechnica.com/business/2015/01/comcast-now-has-more-than-half-of-all-us-broadband-customers/.

293. *Comcast Web Services Terms of Service and Privacy Policy*, COMCAST http://customer.comcast.com/help-and-support/Internet/comcast-web-services-terms-of-service-and-privacy-policy/ (last visited Apr. 15, 2015).

294. Lincoln Spector, *Is Your ISP Spying On You?*, PC WORLD (Sept. 3, 2012, 7:42 AM), http://www.pcworld.com/article/261752/is_your_isp_spying_on_you_.html.

295. *Comcast Customer Privacy Notice*, COMCAST, http://www.comcast.com/Corporate/Customers/Policies/CustomerPrivacy.html (last visited Apr. 15, 2015) ("This information includes which channels, programs, and advertisements are viewed and for how long, for example.").

296. United States v. Comcast Cable Comm., No. 3-03-0553 (M.D. Tenn. 2003).

cable access. The first is the Cable Act of 1992, which strictly defines the information that the cable provider can collect and use.[297] In addition, the Communications Act of 1934, as amended by the Telecommunications Act of 1996, regulates the information that any telecommunication provider can collect and use.[298] One area in which they have improved is encrypting e-mails off its servers to those of another e-mail service provider.[299] There is just simply not enough public information to learn how Comcast thinks of its customers' privacy.

Of the companies on this list, Comcast is the most likely to be considered a state actor on first principles. Comcast owns the infrastructure that allows people to participate in modern day commerce. This can easily be analogized to the interstate highways and even to the company roads in *Marsh v. Alabama*. However, courts that have examined this issue have repeatedly found that ISPs do not function as state actors and therefore cannot violate constitutional rights.[300]

G. CREDO Mobile

CREDO Mobile is a small telecommunications company founded in 1985 that seeks to stimulate progressive change to the leading issues of the day.[301] They have roughly 125,000 subscribers.[302] As one can expect of a company that donates a percentage of every customer's bill to progressive causes,[303] CREDO Mobile is a leading fighter against government invasions of privacy.

---

297. *See* Cable Television Consumer Protection and Competition Act of 1992, 47 U.S.C. § 551 (2012).

298. *See* Communications Act of 1934, 47 U.S.C. § 222 (2012).

299. *Comcast To Encrypt Email After Being Called out by Google,* CIRCA (Nov. 18, 2014, 11:54 AM), http://circanews.com/news/nsa-spying-prompts-encryption-interest.

300. *See, e.g.*, United States v. Richardson, 607 F.3d 357, 364 (4th Cir. 2010) (holding that AOL is not a state actor and the plaintiff could not seek relief for an unreasonable search by AOL); *see also* Steven R. Morrison, *What the Cops Can't Do, Internet Service Providers Can: Preserving Privacy in Email Contents*, 16 VA. J.L. & TECH. 255, 270 (2011).

301. *Our History*, CREDO MOBILE, http://www.credomobile.com/mission/history (last visited Mar. 30, 2015).

302. Lorenzo Franceschi-Bicchierai, *CREDO Mobile Publishes Industry's First Transparency Report*, MASHABLE (Jan. 4, 2014), http://mashable.com/2014/01/09/small-carrier-credo-mobile-publishes-industrys-first-transparency-report/#UikDaa7BPkqo.

303. *Our Mission*, CREDO MOBILE, http://www.credomobile.com/mission/home (last visited Mar. 30, 2015).

On CREDO's transparency website, they state that they "advocate[ ] for the repeal of such statutes that fail to adequately protect the due process rights of its subscribers."[304] In the fourth quarter of 2014, CREDO received three requests for data (that can be made public) and denied two of the requests.[305] These two requests were subpoenas out of the state of Washington.[306] Unfortunately, it is not clear why these requests were denied. In addition, CREDO does not collect or store the content of any communications made by its members.[307] According to CREDO's privacy policy, they do not share subscriber information, except with organizations they partner with to carry out of their progressive goals.[308] They also work with their subscribers to make it easier to communicate with legislators by providing free calling to "speak about these issues."[309]

In addition, it is likely that CREDO was one of the first companies to challenge a National Security Letter.[310] While the name of the actual company was redacted, the Wall Street Journal was able to discover the likely company at the heart of a lawsuit challenging the constitutionality of National Security Letters (NSL).[311] The company challenging the NSL argued that the statute was facially unconstitutional because "[t]he NSL statute violates the anonymous speech and associational rights of Americans by requiring identification of [redacted] without meeting the First Amendment tests, so on its face it violates the associational rights of Americans."[312] The judge agreed with CREDO and enjoined the DOJ from issuing NSLs.[313] The Ninth Circuit vacated and remanded to

304. *CREDO Transparency Report—Q4 2014*, CREDO, http://www.credomobile.com/transparency-previous-reports (last visited Sept. 28, 2016).

305. *Id.*

306. *Id.*

307. *Id.*

308. *Privacy and Security Policy*, CREDO MOBILE, http://www.credomobile.com/privacy (last visited Mar. 30, 2015).

309. *How We Work*, CREDO MOBILE, http://www.credomobile.com/mission/activism (last visited Oct. 23, 2016).

310. Jennifer Valentino-Devries, *Covert FBI Power To Obtain Phone Data Faces Rare Test*, WALL ST. J. (July 18, 2012), http://www.wsj.com/articles/SB10001424052702303567704577519213906388708.

311. *Id.*

312. Petition of Plaintiff [redacted] To Set Aside National Security Letter and Nondisclosure Requirement Imposed in Connection Therewith at 2, *In re* Nat'l Sec. Letter, 930 F. Supp. 2d 1064 (N.D. Cal. Mar. 14, 2013) (No. 11-cv-02173-SI), https://www.documentcloud.org/documents/367100-104697082-us-dis-cand-3-11cv2173-2011-10-02.html.

313. *In re Nat'l Sec. Letter*, 930 F. Supp. 2d at 1081.

the district court due to amendments in the USA Freedom Act and the record was partially unsealed.[314]

CREDO is a different type of wireless company, which seeks to protect the rights of its users. However, CREDO unabashedly supports liberal causes, and this is displayed on their homepage.[315] A conservative may not be happy about spending money on liberal projects. They do have many other choices when it comes to wireless providers and can use many of the other companies. As to whether they would be considered a state actor, a court would find CREDO to be similar to Comcast and is unlikely to consider its actions that of a state actor.

H. Dropbox

Dropbox is a cloud computing company that seeks to centralize all the files of a user or business in one cloud location, which is accessible from any computer in the world.[316] Dropbox mainly competes in the consumer market and according to one source is the leading cloud-computing provider with over 300 million users.[317] As more people migrate their information, previously stored on a physical hard drive within their computer, to cloud services like Dropbox, the government can seek a gag request and search warrant for information on Dropbox, potentially preventing the user from learning of the search.[318] To a user, there is likely to be little distinction between information stored on a Dropbox server and that stored on their hard drive.[319]

In light of a business plan that asks customers to trust Dropbox with their data, Dropbox has enunciated certain principles by which it judges incoming government requests. These four principles are: (1) be transparent by releasing figures for the number of government information requests; (2) fight blanket requests by re-

314. *In re Nat'l Sec. Letter*, No. 13-15957 (9th Cir. Aug. 24, 2015).

315. *See* CREDO MOBILE, http://www.credomobile.com/ (last visited Mar. 30, 2015).

316. *See About Dropbox*, DROPBOX, https://www.dropbox.com/about (last visited Mar. 30, 2015).

317. Erin Griffith, *Who's Winning the Consumer Cloud Storage Wars?*, FORTUNE (Nov. 6, 2014), http://fortune.com/2014/11/06/dropbox-google-drive-microsoft-onedrive/.

318. *See* Douglas Crawford, *Most Dropbox Law Enforcement Requests Want Kept Secret*, BESTVPN (Sept. 12, 2014), https://www.bestvpn.com/blog/10940/most-dropbox-law-enforcement-requests-want-kept-secret/.

319. Dropbox can install a folder on a user's computer that looks just like other folders stored on the hard drive. *See Simple Sharing*, DROPBOX, https://www.dropbox.com/tour/3 (last visited Mar. 30, 2015).

fusing to comply with overly broad requests that are not specific to a person or incident; (3) protect all users by arguing to governments that citizens of one country are entitled to the rights of citizens of every other country; and (4) provide trusted services by designing products without a government backdoor.[320] In addition, Dropbox seeks to protect its users by requiring law enforcement to present a search warrant for the content of a user's files.[321]

As part of Dropbox's commitment to fight back against broad law enforcement requests, it filed an amicus brief, along with many other Internet companies, suggesting that since service providers must comply with warrants issued pursuant to the Secured Communications Act they have an obligation to challenge the validity of those warrants.[322] Dropbox says that they could be sanctioned by a court for failing to comply with a warrant but also be subject to liability for complying with a facially deficient warrant.[323] It is likely that Dropbox has two motives in asserting a right to preemptively challenge a warrant prior to carrying out the warrant. The first is the fear of liability, while the second is to reassure its users that Dropbox seeks to protect their information from government overreach.

Internally, Dropbox uses data to improve its services, but does not sell the data to others.[324] In addition, Dropbox is very clear in its plain English privacy policy that it seeks to treat data as if it is stored on a user's hard drive.[325] These restrictions on data are important as a marketing tactic for Dropbox from a customer relations perspective. If someone thought that by providing information to Dropbox, they would hand over that information to the government, it is likely that no one would sign up for Dropbox.

320. *See Dropbox's Government Data Request Principles*, DROPBOX, https://www.dropbox.com/transparency/principles (last visited Mar. 30, 2015).

321. *2015 Government Transparency Report: July to December 2015*, DROPBOX, https://www.dropbox.com/transparency (last visited Sept. 29, 2016) ("All requests for content information were accompanied by a search warrant, which is the legal standard that Dropbox requires.").

322. Brief for Dropbox Inc. et al. as Amici Curiae Supporting Respondents at 5, *In re* 381 Search Warrants Directed to Facebook Inc. and Dated July 23, 2013, 14 N.Y.S.3d 23 (App. Div. 2015), (No. 30207-13), https://www.dropbox.com/static/Facebook381AmicusBrief.pdf.

323. *Id.* at 13–14.

324. *Dropbox Privacy Policy*, DROPBOX (Sept. 1, 2016), https://www.dropbox.com/terms#privacy.

325. *Id.* ("We believe that our users' data should receive the same legal protections regardless of whether it's stored on our services or on their home computer's hard drive.").

Instead, Dropbox supports changes to privacy law and claims to defend its users against unlawful warrants and subpoenas.

Finally, there are few activities that Dropbox performs that are traditional state functions. In addition, it does not appear that government directs Dropbox in any meaningful way. Therefore, Dropbox is unlikely to fit as a state actor.

I. Internet Archive

The Internet Archive was founded in 1996 to be a modern successor to the Library of Alexandria, which was said to have a copy of every book in the world.[326] It seeks to preserve for posterity websites and online culture to ensure that the work product of millions of individuals will remain for all time.[327] As more information moves to the web from previous media, the Internet Archive has sought to become the library of the future.[328]

In creating this vast archive of the Internet, Internet Archive collects a tremendous amount of data. According to its privacy policy, much of the information it collects is from third parties that donated the information to the Internet Archive.[329] It understands that computer advances may allow for the discovery of privileged information in its archives.[330]

As the Internet Archives' goal is to preserve the past for the future, it seeks to preserve the privacy rights of its users to ensure future donations.[331] It also has gone to battle with the government over National Security Letter (NSL) requests.[332] The Internet Archive was able to get the FBI to withdraw its NSL because the Archive argued that its status as a library limited the FBI's ability to demand its records.[333]

The Internet Archive has specifically limited its exposure and sought to wrap itself in available laws to protect its users from privacy invasions. It does occasionally receive legal process, and ac-

326. *About the Internet Archive*, INTERNET ARCHIVE, http://archive.org/about/ (last visited Apr. 19, 2015).

327. *Id.*

328. *Id.*

329. *Internet Archive's Terms of Use, Privacy Policy, and Copyright Policy*, INTERNET ARCHIVE (Mar. 10, 2001), http://archive.org/about/terms.php.

330. *Id.*

331. *Internet Archive et al v. Mukasey et al*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/cases/archive-v-mukasey (last visited Apr. 19, 2015).

332. Letter from Kurt B. Opsahl, Senior Staff Attorney, Electronic Frontier Foundation, to Special Agent [redacted], FBI (Dec. 17, 2007), https://www.eff.org/document/internet-archive-letter-response-nsl.

333. *See Internet Archive et al v. Mukasey et al*, *supra* note 331.

cording to its Transparency Report, usually provides some information to law enforcement.[334] The limited number of requests compared to other websites makes it hard to generalize on its processes.[335]

It is clear that the Internet Archive understands the role that libraries can play as documenters of the past, and it is a key instrument in a battle over freedom of expression and freedom of association. The Archive has sought to fight against external government requests for information while also limiting its own data collection, which means that governments will have limited incentive to seek information from the Archive.

To determine if the Internet Archive is a private actor, it is most helpful to analogize them to a private university or other grant receiving organization. The question is what percentage of money it receives from government and whether it is directed by governmental agencies.[336] The Internet Archive does in fact receive grant money from the Library of Congress and National Science Foundation.[337] However, its board is made up of independent directors,[338] and while it collaborates with government, it is also a competitor of government.[339] Because of this entwinement, it is possible that a court could find that the Internet Archive does function as a state actor and therefore hold some of its actions to be state actions.

J. Myspace

Myspace was once the world's leading social network site before being eclipsed by Facebook.[340] Today it still has roughly 50

334. In 2014, the Internet Archive received eight requests for user data from United States law enforcement and handed over data in each of the requests. *Law Enforcement Requests,* INTERNET ARCHIVE, http://archive.org/about/faqs.php#Law_Enforcement_Requests (last visited Apr. 19, 2015).

335. *Id.*

336. *See* Reichert v. Elizabethtown Coll., No. CIV.A. 10-2248, 2011 WL 3438318, at *3 (E.D. Pa. Aug. 5, 2011) (holding that the state does not exercise sufficient control over the college).

337. *Credits: Thank You from the Internet Archive*, INTERNET ARCHIVE, http://archive.org/about/credits.php (last visited Apr. 30, 2015).

338. *See Bios*, INTERNET ARCHIVE, http://archive.org/about/bios.php (last visited Apr. 30, 2015).

339. *About the Internet Archive*, *supra* note 326.

340. Mike Shields, *MySpace Still Reaches 50 Million People Each Month*, WALL ST. J.: CMO TODAY (Jan. 14, 2015, 8:00 AM), http://blogs.wsj.com/cmo/2015/01/14/myspace-still-reaches-50-million-people-each-month/.

million unique visitors in the United States.[341] As Myspace was one of the original social media sites, it still contains the remnants of millions of unused accounts, which may have old photographs.[342]

Myspace is the custodian of significant amounts of data that many people have since forgotten about, and therefore they still should seek to protect the privacy of their users. Unfortunately, they do not publish a transparency report nor is the one public instance of them fighting in court against a government request published. According to the EFF, Myspace "provided EFF with a brief from its legal challenge; [EFF] reviewed the case" and determined that it "[met] the standards" EFF had established for designating a company as one that "fought for user privacy in court."[343] Today Myspace actually has a strengthened internal privacy regime since it entered into a consent decree with the FTC over its failure to adhere to its privacy policy statement that it would not share personally identifiable information with advertisers.[344]

It is not clear how carefully Myspace seeks to protect the aged accounts of its users. Myspace clearly is trying to win many of these users back as it redevelops itself as a music website.[345] In addition, they are seeking to leverage their users' registration data to personalize advertisements.[346] They will likely face many of the same internal and external pressures as Facebook and Google as they attempt to redevelop themselves.

Just like Facebook, MySpace also likely could be considered a state actor under the same arguments made above.

341. *Id.* (commenting that many of these users are returning to their accounts in light of the "Throwback Thursday" trend in which the user seeks to post an old photograph on their Instagram or Twitter account).

342. *Id.*

343. Cardozo, *supra* note 149, at 47.

344. Press Release, FTC, Myspace Settles FTC Charges That It Misled Millions of Users About Sharing Personal Information with Advertisers (May 8, 2012), https://www.ftc.gov/news-events/press-releases/2012/05/myspace-settles-ftc-charges-it-misled-millions-users-about.

345. Cynthia Johnson, *Viant, Google, Myspace, and the Future of Advertising*, SEARCH ENGINE J. (Apr. 3, 2015), http://www.searchenginejournal.com/viant-google-myspace-future-advertising/124561/.

346. *Id.*

K. Sonic

Sonic is a small telecommunications company founded by two college friends at Santa Rosa Junior College in 1994.[347] Today they continue to innovate and recently unveiled plans to upgrade their customers to a fiber network.[348] They seek to provide a fast, yet affordable broadband connection to their users.[349] In 2011, Sonic decided to stop storing logs of user data for more than two weeks because Sonic had received a secret court order for the information.[350]

The fight began when the federal government subpoenaed the contents of an e-mail account belonging to WikiLeaks volunteer Jacob Appelbaum.[351] Mr. Appelbaum had become inadvertently a volunteer spokesperson for WikiLeaks but was also a developer for the Tor Project, Inc., which helps "people maintain their anonymity online."[352] Sonic challenged the court order and sought to make its challenge public, or at the very least notify Mr. Appelbaum.[353] Sonic was forced to turn over the contents but was allowed to notify Mr. Appelbaum.[354]

Sonic also publishes a transparency report that shows it provided information to U.S. governments only 24% of the time in 2014.[355] Sonic has sought to make the "[p]rotection of customer privacy . . . [a] core value[ ]."[356] For such a small Internet service provider, their efforts to push back against external pressure are commendable. In addition, their commitment to keeping logs of

347. Julia Angwin, *The Little ISP That Stood Up to the Government*, WALL ST. J.: DIGITS (Oct. 9, 2011, 10:34 PM), http://blogs.wsj.com/digits/2011/10/09/the-little-isp-that-stood-up-to-the-government/.

348. Jeff Baumgartner, *Sonic.net CEO: Tiered Pricing 'Doesn't Make Sense,'* MULTICHANNEL NEWS (June 3, 2014, 12:15 PM), http://www.multichannel.com/news/broadband/sonicnet-ceo-tiered-pricing-doesn-t-make-sense/374915.

349. *About Us*, SONIC, https://www.sonic.com/about-us (last visited Apr. 20, 2015).

350. Angwin, *supra* note 347.

351. Julia Angwin, *Secret Orders Target Email*, WALL ST. J. (Oct. 10, 2011), http://www.wsj.com/articles/SB10001424052970203476804576613284007315072.

352. *Id.*

353. *Id.*

354. *Id.*

355. Dane Jasper, *2014 Transparency Report*, SONIC (Mar. 26, 2015), https://corp.sonic.net/ceo/2015/03/26/2014-transparency-report/.

356. *Id.*

customer data for only short periods of time also shows that they wish to ensure the privacy of their customers.[357]

Sonic is unlikely to be considered a government actor for the same reasons that Comcast is likely to not be considered a state actor.

L. Twitter

Jack Dorsey sent the first tweet on March 21st, 2006 at 3:50 PM.[358] In the fourth quarter of 2014, Twitter had 63 million active U.S. users[359]—roughly 20% of all Americans.[360] There are over 500 million tweets sent each day from a total 288 million global users.[361] That is a tremendous number of tweets from an enormous number of people who are actively viewing and tweeting on a platform that just over a decade ago did not exist. Twitter has become a favorite medium for stockbrokers to communicate with each other and the wider world about their stock picks.[362] In addition, Twitter is often the first site to which people turn to communicate during breaking news stories.[363]

Overseas, Twitter has changed the direction of revolutions by allowing anyone on the street to tweet pictures of events and locations for protests.[364] Users in the United States have adopted Twitter as a tool during such protests as Occupy Wall Street in New York

357. *See Notice to Parties Serving Valid Legal Process on Sonic*, SONIC, https://wiki.sonic.net/images/0/05/Sonic.net_Legal_Process_Policy.pdf (listing Sonic's data retention policies).

358. Jack Dorsey (@jack), TWITTER (Mar. 21, 2006, 3:50PM), https://twitter.com/jack/status/20.

359. Twitter, *Number of Monthly Active Twitter Users in the United States from 1st Quarter 2010 to 4th Quarter 2014 (in Millions)*, STATISTA, http://www.statista.com/statistics/274564/monthly-active-twitter-users-in-the-united-states/ (last visited Apr. 20, 2015).

360. On December 31, 2014, there were approximately 320,088,000 people in the United States. *U.S. and World Population Clock*, U.S. CENSUS, http://www.census.gov/popclock/ (click "Select Date"; then choose "Dec. 31, 2014").

361. *About*, TWITTER, https://about.twitter.com/company (last visited Apr. 20, 2015).

362. Daniel Huang, *Retail Traders Wield Social Media for Investing Fame*, WALL ST. J. (April 21, 2015, 6:30 AM), http://www.wsj.com/articles/retail-traders-wield-social-media-for-investing-fame-1429608604.

363. Amy-Mae Turner, *9 Breaking News Tweets That Changed Twitter Forever*, MASHABLE (Oct. 31, 2013), http://mashable.com/2013/10/31/twitter-news/.

364. Uri Friedman, *Why Venezuela's Revolution Will Be Tweeted*, ATLANTIC (Feb. 19, 2014), http://www.theatlantic.com/international/archive/2014/02/why-venezuelas-revolution-will-be-tweeted/283904/.

City[365] and after the death of Michael Brown in Ferguson, Missouri.[366] This has made data stored on Twitter a target for law enforcement investigating disturbances or other criminal acts that were discussed by tweeting.[367] Often many people leave their tweets public, which means anyone can see them, and these tweets likely have no reasonable expectation of privacy.[368] In addition, the Library of Congress receives a copy of every public tweet to hold for posterity's sake.[369] However, the harder, but still not clear-cut, case is when a user decides to make her tweets private and only available to her friends.

Twitter faces extreme amounts of both types of pressure. In the first instance, Twitter has been subject to and complied with external pressures from foreign governments to withhold content on its website.[370] Twitter received twenty-six removal requests from U.S. federal, state and local governments but did not comply with any of these requests.[371] Twitter also receives subpoenas and warrants for information, as opposed to removal request, from different U.S. governments.[372] From July 1 to December 31, 2014, Twitter received 1622 requests and provided information in 80% of those re-

365. *The Anatomy of the Occupy Wall Street Movement on Twitter*, MIT TECH. REV. (2013), http://www.technologyreview.com/view/516591/the-anatomy-of-the-occupy-wall-street-movement-on-twitter/.

366. Victor Luckerson, *Watch How People Reacted to the Ferguson Decision on Twitter*, TIME (Nov. 25, 2014), http://time.com/3605012/ferguson-twitter-map/.

367. *See, e.g.*, William J. Gorta, *Brooklyn Gang Members Busted After Bragging About Shootings Online*, N.Y. POST (Jan. 20, 2012, 5:20 AM), http://nypost.com/2012/01/20/brooklyn-gang-members-busted-after-bragging-about-shootings-online/.

368. *See* United States v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) ("When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment. However, postings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected.") (citing Katz v. United States, 389 U.S. 347, 351–52 (1967)).

369. Erin Allen, *Update on the Twitter Archive at the Library of Congress*, LIBR. OF CONGRESS BLOG (Jan. 4, 2013), http://blogs.loc.gov/loc/2013/01/update-on-the-twitter-archive-at-the-library-of-congress/.

370. *See, e.g.*, Rebecca Borrison, *Twitter Has Quietly Learned To Censor And Ban Its Users When Governments Ask*, BUSINESS INSIDER (May 25, 2014, 9:05 AM), http://www.businessinsider.com/twitter-censors-political-accounts-2014-5 (showing some instances in which Twitter has acted to remove content at the behest of a foreign government).

371. *Transparency Report: Removal Requests*, TWITTER, https://transparency.twitter.com/removal-requests/2014/jul-dec (last visited Apr. 21, 2015).

372. *Transparency Report: United States: Information Requests*, TWITTER, https://transparency.twitter.com/country/us (last visited Apr. 21, 2015).

quests.[373] This is a comparable number to many of the companies above. Unfortunately, Twitter does not break down whether it complied more with search warrants as opposed to subpoenas.[374] Like most companies on the EFF's list that fought against the government in court, they do require a search warrant for content.[375]

In addition, Twitter has also filed suit in court to protect the privacy of their users. In one case surrounding the investigation into the leaks of Chelsea Manning published on WikiLeaks.org, Twitter sought to unseal a court order asking for information about a subscriber to notify the subscriber.[376] Twitter was able to notify the subscriber who appealed the decision to block access to the underlying court order.[377] The Fourth Circuit Court of Appeals agreed with the Magistrate Judge and found that the government's interest in keeping the court order secret outweighed the right of the public and the subscriber to understand the contents.[378]

In another case related to Occupy Wall Street, Twitter notified a subscriber that it had received a subpoena for the content of his tweets.[379] The subscriber filed a motion to quash the subpoena, which was denied for lack of standing.[380] Twitter has since changed its privacy policy to give users a proprietary interest in their tweets to give them standing.[381] Twitter then filed its own motion to quash the subpoena, which was again denied.[382] In that case, Twitter argued that public tweets should be protected from the government and require a search warrant.[383] The court found that, according to the Stored Communications Act, the records stored at Twitter can be subpoenaed, and therefore Twitter was under an obligation to turn over the records.[384] Twitter attempted to appeal the decision

373. *Id.*

374. *Id.*

375. *Guidelines for Law Enforcement*, TWITTER, https://support.twitter.com/entries/41949#8 (last visited Apr. 22, 2015).

376. *In re* Application of the United States for an Order Pursuant to 18 U.S.C. Section 2703(D), 707 F.3d 283, 287–88 (4th Cir. 2013).

377. *Id.* at 288.

378. *Id.* at 295.

379. *See* People v. Harris, 949 N.Y.S.2d 590, 591 (Crim. Ct. 2012), *aff'd*, 971 N.Y.S.2d 73 (Table) (App. Div. 2013).

380. *See id.* at 598.

381. Tara M. Breslawski, Case Note, *Privacy in Social Media: To Tweet or Not To Tweet?*, 29 TOURO L. REV. 1283, 1284 (2013).

382. *Harris*, 949 N.Y.S.2d at 592.

383. *Id.*

384. Memorandum in Support of Non-Party Twitter, Inc.'s Motion To Quash § 2703(D) Order, *Id.* at 2. Congress has yet to fix the problem first identified by a circuit court in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), that the

but was forced to turn over the records "begrudgingly" before the appeal.[385]

Twitter also is subject to pressure from its user base to take a more proactive role in challenging the behavior of cyberbullies online and recently announced a new policy to create an automated system to discover "abusive content."[386] Twitter's CEO has acknowledged that it has not done enough to combat trolling, or as he put it in an internal memo, "[w]e suck at dealing with abuse and trolls on the platform and we've sucked at it for years."[387]

Twitter's general counsel, Vijaya Gadde, published an op-ed to discuss Twitter's strategy in handling abusive content.[388] She argued that Twitter understands that "[i]t is not our role to be any sort of arbiter of global speech."[389] But, she also wrote that Twitter must take a more active role in policing the line between abuse and free speech.[390] This is the same line that U.S. government has been trying to police for decades. Whether Twitter would seek to recognize the First Amendment rights of users on its website, it can look towards the First Amendment as a guide in determining how to draw a correct line.

Electronic Communications Privacy Act does not require a warrant for e-mail content that is stored longer than 180 days on a cloud computer. *Id.* at 283. The Court in *Warshak* found that investigators must seek a warrant for such content, but this holding is currently limited to only the Sixth Circuit. Congress' failure is further highlighted by the Department of Justice's adoption of a policy that requires a search warrant when an investigator seeks the content of e-mails. *ECPA (Part 1): Lawful Access to Stored Content: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec., & Investigations of the H. Comm. on the Judiciary,* 113th Cong. 16, 20 (2013) (statement of Elana Tyrangiel, Acting Assistant Att'y Gen., Office of Legal Policy, Department of Justice) ("We agree, for example, that there is no principled basis to treat email less than 180 days old differently than email more than 180 days old."); *see also* Timothy B. Lee, *Eric Holder endorses warrants for e-mail. It's about time.* WASH. POST (May 16, 2013) (describing Attorney General Eric Holder's testimony that the government must receive a warrant before reading American's email).

385. Breslawski, *supra* note 381, at 1303.

386. Shreyas Doshi, *Policy and Product Updates Aimed at Combating Abuse*, TWITTER BLOG (Apr. 21, 2015, 10:57 AM), https://blog.twitter.com/2015/policy-and-product-updates-aimed-at-combating-abuse.

387. Nitasha Tiku & Casey Newton, *Twitter CEO: 'We suck at dealing with abuse,'* VERGE (Feb. 4, 2015, 9:25 PM), http://www.theverge.com/2015/2/4/7982099/twitter-ceo-sent-memo-taking-personal-responsibility-for-the (referencing memo written by Twitter's CEO, Dick Costolo to Twitter employees).

388. Vijaya Gadde, *Twitter Executive: Here's How We're Trying To Stop Abuse While Preserving Free Speech*, WASH. POST (Apr. 16, 2015), http://www.washingtonpost.com/posteverything/wp/2015/04/16/twitter-executive-heres-how-were-trying-to-stop-abuse-while-preserving-free-speech/.

389. *Id.*

390. *Id.*

Since Twitter is a direct competitor of Facebook, the same state actor analysis above would apply to Twitter.

M. Yahoo

"Yet Another Hierarchical Officious Oracle," or Yahoo, was founded in 1994 as a searchable index of pages and, like many of the companies on this list, has gone through recent troubles competing with Google.[391] Marissa Mayer, a former Google executive, took over Yahoo in 2012 with the intentions to lead it back to its original strength.[392] While still disappointing many Wall Street analysts, Yahoo is beginning to find its competitive advantage.[393] It has revitalized its search results through a deal with Microsoft and is seeking to develop its own ad platform.[394]

In addition, Yahoo executives have put together plans to try to capitalize on the age of many Yahoo products.[395] For instance, many users have had e-mail accounts with Yahoo for over twenty years, and there remains a large amount of data stored in these accounts.[396] An anonymous source explained how Yahoo seeks to use this historical data. For instance, if a user has sent many e-mails about a certain baseball team to his friends, "Yahoo will scan[ ] that user's inbox . . . [and] know to keep that user abreast of everything going on with that baseball team."[397] This creates the potential for some type of privacy invasion but is likely similar to Google's Gmail, which scans e-mails to provide relevant advertising.[398]

One of Yahoo's acquisitions over the years, Tumblr, is a blogging network which allows its users to post almost anything onto a public website.[399] As part of Tumblr's independent privacy policy, it states, "[d]on't be afraid to share amazing things, but do under-

391. Simon Holland, *Yahoo: An 18-year Timeline of Events*, PERFORMANCEIN (July, 17, 2012), http://performancein.com/news/2012/07/17/yahoo-18-year-timeline-events/ (last visited Apr 24, 2015).

392. *Id.*

393. Vindu Goel, *Yahoo Shows Growth in Mobile Advertising, but Results Miss Estimates*, N.Y. TIMES (Apr. 21, 2015), http://www.nytimes.com/2015/04/22/technology/yahoo-quarterly-earnings.html.

394. Jon Fingas, *Microsoft and Yahoo Can End Their Search Deal After October 1st*, ENGADGET (Apr. 21, 2015), http://www.engadget.com/2015/04/21/microsoft-and-yahoo-can-end-search-deal/.

395. Nicholas Carlson, *Inside Marissa Mayer's Plan To Take on Google*, BUSINESS INSIDER (Apr. 22, 2015, 1:22 PM), http://www.businessinsider.com/marissa-mayers-plan-to-take-on-google-is-code-named-index-2015-4.

396. *Id.*

397. *Id.*

398. *See* Gibbs, *supra* note 209.

399. TUMBLR, https://www.tumblr.com/ (last visited Apr. 24, 2015).

stand that it can be hard to completely remove things from the Internet once they've been reblogged a few times."[400] It is clear that Tumblr seeks to become an organized website that can act as the bulletin boards of older generations. As part of that goal, Tumblr has community guidelines, which seek to protect their users' freedom of speech.[401] As everything posted on Tumblr is public, these guidelines seek to regulate public speech by aligning with the First Amendment's freedom of speech.

Yahoo, like many other websites, believes that the key to its success is its users' trust. As Marissa Mayer is quoted on Yahoo's transparency page, "We've worked hard over the years to earn our users' trust and we fight hard to preserve it."[402] According to their transparency report for the second half of 2014, out of a total of 4865 requests, Yahoo provided non-content information in 59% and content in 24% of these requests.[403] They rejected 5% of requests and found no information in another 12% of requests.[404] The number of complied requests is a little higher than some of their peer companies.

As part of Yahoo's transparency report, they outline three goals to protect their users.[405] The first is to protect user data through heightened standards for law enforcement, encryption of communications including e-mail, and mentorship of newer start-up companies.[406] The second is to advocate for their users by both advocating for intelligence overhaul bills and challenges to government court orders, including the fact that they were the only company to challenge "the predecessor to Section 702 of the FISA Amendments Act in the secret Foreign Intelligence Surveillance Court [(FISC court)]."[407] While the Court ruled in favor of the government, in Yahoo's brief before the FISC court, Yahoo said that it was seeking to protect the "Fourth Amendment rights of its custom-

400. *Privacy Policy*, TUMBLR (Jan. 27, 2014), https://www.tumblr.com/policy/en/privacy.

401. *Community Guidelines*, TUMBLR (Jan. 26, 2015), https://www.tumblr.com/policy/en/community ("As a global platform for creativity and self-expression, Tumblr is deeply committed to supporting and protecting freedom of speech.").

402. *Transparency Report: Overview*, YAHOO, https://transparency.yahoo.com/ (last visited Apr. 24, 2015).

403. *Transparency Report*: *Government Data Requests*, YAHOO, https://transparency.yahoo.com/government-data-requests?tid=19 (last visited Sept. 29, 2016).

404. *Id.*

405. *Transparency Report: Users First*, YAHOO, https://transparency.yahoo.com/users-first/index.htm (last visited Apr. 24, 2015).

406. *Id.*

407. *Id.*

ers and subscribers against a program of warrantless surveillance."[408] Yahoo's constitutional argument started from an agreed-upon statement that "U.S. persons using Yahoo! services have legitimate expectations of privacy in their [redacted] communications, even when such persons are located overseas."[409] Yahoo clearly sees the content of communications as something that must be entitled to basic Fourth Amendment protections and for which users are entitled to a legitimate expectation of privacy.

The final goal is for Yahoo to promote basic human rights including freedom of expression and a right to privacy.[410] As part of this plank, Yahoo has created the Yahoo Business & Human Rights Program, which focuses on external pressures against Yahoo from governments.[411] While Yahoo seems to be very focused on protecting its users from external pressures, it is not all together clear if it has comprehensive policies in place to protect its users from internal pressures.

For the same reasons that Google and Microsoft would not likely be considered state actors, a court would be unlikely to find that Yahoo was a government actor.

V.
HEIGHTENED LEVEL OF SCRUTINY FOR CORPORATE ACTION

While it is unlikely that many of the above corporations would be considered public actors under current doctrine, that does not mean that the ethos underlying constitutional due process standards should not apply to them. These companies all have the ability to cause a privacy invasion or censor individuals and cause them harm. The same reasons that underlie the protections in the First and Fourth Amendment can apply against companies.

Corporations, which have the power necessary to invade privacy, often get away with more invasions of privacy than the government. Often, they can use necessity and functionality as an excuse to require more information. In addition, many of these corporations are built on using data to sell better, more targeted ads, which in turn provides money for more features. To truly tackle privacy

408. Brief for Yahoo at 8, Yahoo v. United States, No. 08-01 (FISA Ct. Rev. 2008), https://cdt.org/files/2014/09/1-yahoo702-brief.pdf.

409. *Id.* at 30.

410. *Transparency Report: Users First*, *supra* note 405.

411. *Yahoo Business & Human Rights Program*, YAHOO, http://yahoobhrp.tumblr.com/post/75544734087/yahoo-business-human-rights-program-yahoo (last visited Apr. 24, 2015).

issues in the future, the artificial buffer between government surveillance and corporate surveillance must be pulled down by policymakers. Requiring corporations to respect the First Amendment or Fourth Amendment rights of their users likely would cost billions and may detract from further innovation. Nonetheless, it is a conversation worth having.

Unfortunately, Congress is unwilling and unlikely to pass any comprehensive privacy reform package.[412] Even if it were to pass such a proposal, there is the possibility that it would fail to address many of the privacy problems associated with Big Data. President Obama recently released a consumer bill of rights for which there is little likelihood of passage.[413] Even if the bill were to pass, the bill does not provide adequate and appropriate safeguards to prohibit a company from examining a user's content or censoring his or her speech on its website. In today's Internet age, both the government and the corporation have equivalent ability to cause harm. In fact, corporations may prove more harmful on an everyday basis than the government. In addition, there are certain due process requirements that the government must acknowledge in order to invade the privacy of an individual. For instance, they may need to receive a warrant or allow for the individual to challenge a subpoena before a neutral decision maker. None of these procedural due process requirements apply to a private corporation.

As websites delve deeper into Big Data and harness all of its potential, they must be cognizant of how their actions as corporations can have an effect on individuals. There are some companies that would likely be happy to look the other way and continue with the fiction that their actions should not be held as equivalents of government actions. There are other companies that seek to be model corporate citizens and lead in the field of privacy rights. These are the companies that must be cognizant of their impact on the free speech and privacy rights that all Americans associate with being an American. These corporations must recognize that their actions can chill speech or prevent a group from assembling.

---

412. In 2011, former Chairman Patrick Leahy of the U.S. Senate Judiciary Committee first proposed a fix to ensure that the government receives a warrant to search the contents of e-mail communications. *See* Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011). This bill was voted out of committee in 2013, but has yet to pass the Senate, even though it is thought to have wide support. Electronic Communications Privacy Act Amendments Act of 2013, S. 607, 112th Cong. (2013).

413. Brendan Sasso, *Obama's 'Privacy Bill of Rights' Gets Bashed from All Sides*, NAT'L J. (Feb. 26, 2015, 1:11 PM), http://www.nationaljournal.com/tech/obama-s-privacy-bill-of-rights-gets-bashed-from-all-sides-20150227.

While the courts have spent years developing constitutional doctrines to curb violations of the First or Fourth Amendment, companies often do not have these same or similar safeguards in place. If the corporation must invade one of these extremely important rights, it ought to consider its actions under a heightened level of scrutiny,[414] akin to the Court's strict scrutiny test in the First Amendment context or reasonable expectation of privacy test in the Fourth Amendment context, before it engages in any invasion of traditionally protected constitutional rights. A high-level employee could play the role of a judge and decide whether the compelling corporate interest outweighs the violation of the fundamental right. Companies can use the underlying rationales of both of these general tests to evaluate their own new general policies or individual actions. They can do this by ensuring that the invasion of rights is narrowly tailored to achieve a compelling interest.[415]

The Supreme Court has found that:

> [G]overnment may impose reasonable restrictions on the time, place, or manner of protected speech, provided the restrictions "are justified without reference to the content of the regulated speech, that they are narrowly tailored to serve a significant governmental interest, and that they leave open ample alternative channels for communication of the information."[416]

When a company is looking to evaluate new community guidelines or seeking to take action against a potential website abuser, it should look to this test to justify its guidelines. Companies should commit to the "bedrock principle underlying the First Amendment . . . that the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable."[417] While Internet companies may not feel the same re-

414. The concept that different levels of scrutiny apply to different legislation was first introduced in the famous footnote 4 of *United States v. Carolene Products*, in which Justice Stone for the Court stated that "prejudice against discrete and insular minorities may be a special condition, which tends seriously to curtail the operation of those political processes ordinarily to be relied upon to protect minorities, and which may call for a correspondingly more searching judicial inquiry." United States v. Carolene Prods. Co., 304 U.S. 144, 152 n.4 (1938).

415. *Cf.* Parents Involved in Cmty. Sch. v. Seattle Sch. Dist. No. 1, 551 U.S. 701, 720 (2007) (applying the Supreme Court's current strict scrutiny formulation in the affirmative action context).

416. Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989) (quoting Clark v. Cmty. for Creative Non-Violence, 468 U.S. 288, 293 (1984)).

417. Texas v. Johnson, 491 U.S. 397, 414 (1989).

quirement to give a soapbox to all offensive individuals, they should be mindful of the role that they have in policing the avenues of speech in modern America. The Supreme Court has outlined limited exceptions to the general content-neutral requirement in *United States v. Alvarez*.[418] These categories are: "advocacy intended, and likely, to incite imminent lawless action, obscenity, defamation, speech integral to criminal conduct, so-called 'fighting words,' child pornography, fraud, true threats, and speech presenting some grave and imminent threat the government has the power to prevent."[419] If speech does not fall into any of these categories, the website should ensure that its employees do not censor the individual without providing sufficient due process. This should at a minimum include an opportunity to contest the distinction and an appeals process to an attorney.

Finally, companies must remain aware that in instituting certain automated advertising they may chill free speech by potentially preventing people from sharing on their forums. A company should make clear in their privacy policy that no human will ever see the results of the advertising and that computers do all the internal processing. If a human, for instance, spot checks to ensure quality control, the company should ensure that its employees do not have access to any personally identifiable data. In addition, the company should educate these employees in basic First Amendment values to ensure that they do nothing to stifle free speech.

In determining when a human at a company should examine the contents of a user's private information, companies ought to look at the reasonable expectation of privacy standard elaborated on by the Supreme Court.[420] Microsoft has proposed a series of rules in which it decides when it is appropriate to examine the contents of one of its e-mail accounts.[421] These steps can provide a strong framework that every Internet company should adopt any time it decides, with human eyes, to examine the contents of an e-mail or document stored on its site. A model set of instructions for a company to adopt would look similar to below:

---

418. United States v. Alvarez, 132 S. Ct. 2537, 2544 (2012).

419. *Id.* (citations omitted).

420. *See, e.g.*, Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) ("[A] person has a constitutionally protected reasonable expectation of privacy."); *see generally* Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700 (2010) (exploring the issues associated with Fourth Amendment seizure doctrine in the context of computer data).

421. *Infra* Part II: Microsoft.

1. Company A will honor the privacy of their users by requiring the below process before it would conduct a search that would ordinarily require a court order.

2. Company A will create a document which includes the probable cause to believe that a crime or other serious infraction has been committed with the use of an account on the company's website and the particular account that it wishes to search.

3. Company A will submit this document to an independent lawyer who should have full and ultimate authority to deny or alter the request based on prevailing legal doctrine in the jurisdiction in which the crime or other serious infraction would likely be prosecuted.

4. Company A will conduct the search to look for the information it specified in its application and report to the independent lawyer any potential deficiencies in the search.

5. Company A will notify their user within 30 days of the search of the account and provide the probable cause for the search. This can be repeatedly extended for 30 days if the company believes it reasonably necessary to protect the company and makes this showing to an independent lawyer.

This process may seem onerous, but it would go very far in restoring the users' faith in a service. An exception would likely have to be made that a computer can examine the contents so long as the computer does not transmit that information to a third party. All processing of information would have to occur within the company's servers.

VI.
CONCLUSION

Big Data is a key building block for many of the most innovative and disruptive companies in the world. It is allowing Internet titans such as Google to invest in projects that seek to leave the world a better place. Companies ought to think beyond just their bottom line and ensure that in the United States they actively protect and defend certain rights that Americans have fought to enjoy. Even if courts do not find that they are state actors, they can incorporate these rights into their ethos and community guidelines.