Pace Law Review

Volume 35
Issue 1 *Fall 2014*
Symposium: Social Media and Social Justice

Article 11

September 2014

Social Media and the Internet: A Story of Privatization

Victoria D. Baranetsky

Social Media and the Internet: A Story of Privatization

Victoria D. Baranetsky*

I. Introduction

Since the 1980s various parts of the United States government — from small-town task forces to our country's most important federal agencies — were transferred from public to private oversight.[1] In some ways, this turn toward privatization had positive effects. For example, unwieldy state programs became faster, cheaper, and more efficiently run.[2] However, the shift also came with costs. Ten years ago, Dean of Harvard Law School, Martha Minow, observed in a *Harvard Law Review* article that the turn toward the private realm put

* Victoria D. Baranetsky. First Amendment Fellow at the New York Times Company, Harvard Law School, J.D. 2011. I would like to thank Robert Horning for his comments and critiques. All reflections and opinions are, of course, my own and do not speak for anyone else or any other entity, including The New York Times Company. Thank you also to The Pace Law Review editors who shepherded this article to publication.

1. The Reagan and Bush Administrations were in large part responsible for ushering in this process, following the lead of Margaret Thatcher and her widespread reforms in the United Kingdom. *See* Margaret Thatcher, *Margaret Thatcher: Rebuilding an Enterprise Society Through Privatisation*, REASON FOUND. (Jan. 1, 2006), http://reason.org/news/show/apr-2006-margaret-thatcher-reb. Thatcher believed that most governments, after both World Wars, had overextended themselves into the private realm and her answer to this malady was to withdraw government from industry, manufacturing, and even some traditional governmental functions. Ronald A. Cass, *Privatization: Politics, Law and Theory*, 71 MARQ. L. REV. 449, 449-523 (1988). The traditional government functions test for cases of federalism had its genesis in the case, *National League of Cities v. Usery*, 426 U.S. 833 (1976). The test is still used today. *See, e.g.*, United Haulers Ass'n v. Oneida-Herkimer Solid Waste Mgmt. Auth., 550 U.S. 330, 345 (2007) (plurality opinion).

2. In Philadelphia, for instance, Governor Ed Rendell saved $275 million by privatizing forty city services – generating more than $3 billion. Russell Nichols, *The Pros and Cons of Privatizing Government Functions*, GOVERNING MAG. (Dec. 2010), http://www.governing.com/topics/mgmt/pros-cons-privatizing-government-functions.html.

many individuals' civil rights and civil liberties in jeopardy.[3]

Today, the same concern exists with another public arena gone private – the Internet. As this article will explain, the Internet was in large part created by the United States government as a military tool of defense to collect, store, and decentralize information. But eventually, as the federal government receded from its role in overseeing the Internet, private entities began to enter the landscape, leaving potential civil rights and civil liberties violations without a constitutional remedy. Unlike other fora, the stakes are arguably higher with the Internet because its fundamental public function involves a public resource replete with private information – digital data.[4]

In an article written nearly a decade ago, Yochai Benkler gave a similar account. Benkler argued that the Internet was a neglected commons where tracks of public grazing had disappeared because government had abstained "from designating anyone as having primary decision-making power over use of . . . [the] resource."[5] This article suggests a related but distinct idea: that through its abstention the government has privatized the Internet, but still holds a substantial stake in how private companies collect information over the network.

In June 2013, government contractor Edward Snowden leaked a cache of top-secret documents revealing operational details about the U.S. National Security Agency (NSA) and its global surveillance programs. It is now well-documented that the government engages in surveillance by requesting information from private databases. Companies like Microsoft, Facebook, Google, Apple and other Silicon Valley corporations, that collect data for profitmaking purposes, provide information to federal and state officials for law enforcement

3. "[P]rivatization potentially jeopardize[s] public purposes by pressing for market-style competition, by sidestepping norms that apply to public programs, and by eradicating the public identity of social efforts to meet human needs." Martha Minow, *Public and Private Partnerships: Accounting for the New Religion*, 116 HARV. L. REV. 1229, 1230 (2003).

4. In the midst of writing this paper, the President's commission issued a paper which suggested that private corporations wielding public data require some new type of regulation. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014).

5. Yochai Benkler, *The Commons as a Neglected Factor of Information Policy*, 26th Annual Telecommunications Policy Research Conference (Oct. 3, 1998).

purposes.

In response, some corporations argued that this transaction was ostensibly protected under the First Amendment. However, eventually many tech companies, and public officials became openly critical of the government's protocol. Starting in December 2013, Google, Facebook, Apple, Microsoft, Twitter, Yahoo, LinkedIn, and AOL issued an open letter to the White House and members of Congress enumerating a set of reform principles to better safeguard the information of Internet users.[6] Subsequently, the House voted in an overwhelming vote of 303-to-121 to curtail the sweeping collection of telephone records conducted by the NSA.[7]

Silicon Valley organizations were also criticized for "complying" with government demands.[8] In April, European politicians chastised Google for "colluding" with government agencies and expanding into the sphere of government.[9] By May, the European Court of Justice upheld the "right to be forgotten," which demands companies comply with more stringent privacy protections. That same month, the Obama Administration released a report suggesting regulations to be placed on private companies for data use.[10] "There is a role for

6. Letter from Google, Facebook, Apple, Microsoft, Twitter, Yahoo!, LinkedIn, Dropbox, AOL, to the U.S. Senate (Oct. 31, 2013). A shorter version of the letter appeared in full-page ads in several print publications, including *The New York Times*, the *Washington Post*, *Politico*, *Roll Call* and *The Hill*.

7. "[T]he House's 303-to-121 vote on the U.S.A. Freedom Act sent a signal that both parties were no longer comfortable with giving the NSA unfettered power to collect records in bulk about Americans." Jonathan Weisman & Charlie Savage, *House Passes Restraints on N.S.A.'s Data Mining*, N.Y. TIMES, May 23, 2014, at A14 (reporting the House of Representatives overwhelmingly voted to rein in the National Security Agency by a vote of 293 to 123, approving a proposal by Reps. James Sensenbrenner (R-WI), Thomas Massie (R-KY), Zoe Lofgren (D-CA), and others that would limit "backdoor searches" – a method of spying on Americans despite legal safeguards).

8. Claire C. Miller, *Tech Companies Concede to Surveillance Program*, N.Y. TIMES, June 8, 2013, at A12.

9. Alison Smale, *In Germany, Strong Words from Publisher over Google's Power*, N.Y. TIMES, April 17, 2014, at B2.

10. EXEC. OFFICE OF THE PRESIDENT, *supra* note 4. The report makes six policy recommendations; including passing a national data breach law that would require companies to report major losses of personal and credit card data, seeking legislation that would define consumer rights, extending privacy protections to individuals who are not citizens of the United States,

government to hold companies accountable and establish incentives," said Edward W. Felten, former chief technologist of the Federal Trade Commission.[11] "There needs to be enough incentive for companies to do the hard work."[12] However, this article observes that both corporations and the government are compromised by their incentives to continue collecting data.

Recently, technology companies have made some effort, even if mostly superficial, to change their privacy protocols. For example, Facebook created a cartoon dinosaur mascot on the site to make users more aware of their sharing preferences.[13] In addition, companies like Google, Facebook, Amazon, and Twitter publicly stated that privacy policies must be reformed.[14] However, most companies stated that reform had to start from the government.[15]

This immobilization is unsurprising. Big Data has become big business.[16] As McKinsey & Company recently stated, "Big Data is 'the next frontier for innovation, competition, and productivity.'"[17] It is "one of the leading topics on executive

and ensuring that data collected about students is used only for educational purposes. But most significantly, the report finds that data can be used in subtly discriminatory ways — to make judgments, sometimes in error, based on race, age, and sex. The report states "that the same technology that is often so useful in predicting places that would be struck by floods or diagnosing hard-to-find illnesses in infants also has 'the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education and the marketplace.'" David Sanger & Steve Lohr, *Call for Limits on Web Data of Customers*, N.Y. TIMES, May 1, 2014, at A1.

11. Sanger & Lohr, *supra* note 10.

12. *Id.*

13. *See* Nick Bilton, *Facebook's New Privacy Mascot: The Zuckasaurus*, N.Y. TIMES, May 23, 2014, at B1; Robert Horning, *No Life Stories*, NEW INQUIRY (July 10, 2014), http://thenewinquiry.com/essays/no-life-stories/.

14. For instance, Google has said it will work to build encryption systems that can defeat NSA spying, and several companies have revised their policies to say they will warn customers when the government tries to subpoena relevant data stored on them. Sanger & Lohr, *supra* note 10.

15. *Id.*

16. Jonathan Shaw, *Why "Big Data" is a Big Deal*, HARV. MAG. (Mar.–Apr. 2014), http://harvardmagazine.com/2014/03/why-big-data-is-a-big-deal.

17. Brooks Bell, *How Soon Will Big Data Yield Big Profits?*, FORBES MAG. (Nov. 12, 2013, 9:09 AM), http://www.forbes.com/sites/techonomy/2013/11/12/how-soon-will-big-data-yield-big-profits/.

agendas and a driver of technology."[18] A new field of professionals, called data brokers, makes incredible proceeds by collecting and selling particularized consumer information.[19] By 2016, today's $6 billion data industry is projected to almost quadruple to $23.8 billion.[20]

This data-driven economy has led to some extreme behavior. Several social media companies have changed their business models from passive data collection to actively conducting experiments on users in order to collect more information. In June of 2014, Facebook "disclosed that it had tested to see if emotions were contagious [by] deliberately manipulating the emotional content of the news feeds for 700,000 people."[21] OKCupid, a dating website, published

18. Dan Vesset & Henry Morris, *Unlocking the Business Value of Big Data: Infosys BigDataEdge*, IDC, Feb. 2013, at 1; Shaw, *supra* note 16 ("There is a movement of quantification rumbling across fields in academia and science, industry and government and nonprofits . . . . It is hard to find an area that hasn't been affected.").

19. Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA (June 13, 2014, 1:59 PM), http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you. One of these companies alone has "multi-sourced insight into approximately 700 million consumers worldwide," and another asserts its data "includes almost every U.S. household." Office of Oversight And Investigations Majority Staff, A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes (2013) ("Some of the companies maintain thousands of data points on individual consumers, with . . . a list of approximately 75,000 individual data elements that are in [a] system.").

20. In fact, entire new business models are being built in response. James Platt et al., *Seven Ways to Profit from Big Data as a Business*, BCG.PERSPECTIVES (Mar. 05, 2014), https://www.bcgperspectives.com/content/articles/information_technology_strategy_digital_economy_seven_ways_profit_big_data_business/. The news business, for instance, has seen a recent trend toward data-driven reporting exemplified by the work of FiveThirtyEight.com, headed by Nate Silver; and Vox.com, led by former policy blogger Ezra Klein. The trend has even inspired older publishers like *The New York Times*, *The Wall Street Journal*, and *The Guardian* to get on board. *The New York Times*' "The Upshot" has recently made waves in the news industry with its new data-driven reporting. David Leonhardt, *Navigate News with the Upshot*, N.Y. TIMES (Apr. 22, 2014), http://www.nytimes.com/2014/04/23/upshot/navigate-news-with-the-upshot.html?abt=0002&abg=0; see Mark Sweney, *The Guardian Appoints Alberto Nardelli as Data Editor*, GUARDIAN (July 3, 2014), http://www.theguardian.com/media/2014/jul/03/guardian-alberto-nardelli-data-editor-tweetminster.

21. Molly Wood, *Looking for Love on the Web, as It Experiments with*

results of three experiments it ran on its users.[22] The company's president subsequently stated, "If you use the Internet, you're the subject of hundreds of experiments at any given time, on every site. . . . That's how websites work."[23]

While private companies profit from collection of data, federal and state governments openly rely on private hands to gather information for law enforcement purposes. In a recent report, the White House stated, "data is a national resource," and "[it] should be made broadly available to the public wherever possible, to advance government efficiency, ensure government accountability, and generate economic prosperity and social good."[24] This mutually supportive structure was embodied last year when the Obama Administration invited Silicon Valley representatives to D.C. to work together on the issue of waning public trust.[25]

With companies incentivized to continue collecting more personal information and the government incentivized to keep regulation of the private sphere at the status quo, law enforcement surveillance of more private information seems to be the likely consequence. Constitutionally speaking, this raises fundamental concerns about privacy. Are constitutional rights, such as the Fourth Amendment's protection against unwarranted searches and seizures, abrogated in these circumstances? Are companies like Microsoft, Facebook, Google and Apple, acting as a privatized arm of the government, when they turn over information collected for commercial purposes? If so, does state action apply?

Under the Fourth Amendment, the U.S. Constitution protects privacy by prohibiting government officials from

You, N.Y. TIMES, July 29, 2014, at B1.

22. *Id.*

23. *Id.*

24. EXEC. OFFICE OF THE PRESIDENT, *supra* note 4, at 67.

25. For example, in late 2013 and early 2014, the President met at the White House with several Silicon Valley executives to discuss privacy issues and data collection. *See, e.g.*, Jackie Calmes & Nick Wingfield, *Tech Leaders and Obama Find Shared Problem: Fading Public Trust*, N.Y. TIMES, Dec. 17, 2013, at B1; David S. Joachim, *Obama and Tech Executives to Meet Again on Privacy Issues*, N.Y. TIMES, Mar. 21, 2014, http://www.nytimes.com/2014/03/22/technology/obama-and-tech-executives-to-meet-again-on-privacy-issues.html?_r=0.

performing unreasonable searches and seizures.[26] However, central to invoking the Fourth Amendment protection, an individual must be affected by a "state action," an action made by employees of the federal or state government.[27] Therefore, a question remains whether Fourth Amendment violations occur when companies break the direct link between government and citizen. In addition, the individual must have a reasonable expectation of privacy which the Supreme Court has held does not exist if a person "knowingly exposed" information to a third party — such as a social media website or an internet provider.[28]

Given these concerns, many areas of government have called for reform. A recent White House report, stated "[users' data should] be accorded stronger privacy protections than they are currently."[29] The Supreme Court in *Riley v. California*[30] unanimously held that police may not, without a warrant,

26. U.S. CONST. amend. IV. The First Amendment protects an employee's freedom of speech and association. U.S. CONST. amend. I. The Fifth Amendment ensures against self-incrimination and the Fourteenth Amendment guarantees due process and equal protection. U.S. CONST. amend. V, XIV.

27. Under the "state action" doctrine, no privacy protections may be afforded where data is collected by wholly private companies. U.S. CONST. amend IV; 42 U.S.C. § 1983 (2012).

28. A reasonable expectation of privacy exists if there is a) a subjective expectation of privacy and b) that expectation is one that society as a whole would think is legitimate. Lugar v. Edmonson Oil Co., 457 U.S. 922, 928-29 (1982). *See* Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 563 (2008) ("By disclosing to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed. . . . 'In other words, a person cannot have a reasonable expectation of privacy in information disclosed to a third party.'" (quoting *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). "Most information a third party collects — such as your insurance records, credit records, bank records, travel records, library records, phone records and even the records your grocery store keeps when you use your 'loyalty' card to get discounts — was given freely to them by you, and is probably not protected by the Fourth Amendment under current law." *Reasonable Expectation of Privacy*, Surveillance Self-Defense Project 1, https://ssd.eff.org/your-computer/govt/privacy (last visited Nov. 19, 2014)

29. The White House Report considers whether private companies' "Terms of Service" "still allows us to control and protect our privacy as the data is used and reused." Sanger & Lohr, *supra* note 10. Other branches of government have echoed this worry.

30. Riley v. California, 134 S. Ct. 2473 (2014) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

search digital information on a cellphone seized from an arrested individual. The Court reasoned that "mobile application software on a cell phone, or 'apps,' offer a range of tools for managing detailed information about all aspects of a person's life."[31]

The public agrees. A Pew Research survey, released last September, reported that a majority of Americans worry about their privacy.[32] About 86% took some steps to remove their digital footprint.[33] "But these efforts are often insufficient because companies have multiple ways to monitor people, some of which are very hard to evade."[34]

In line with these inquiries, this article will question what role private and public actors assume in the current structure of data collection and what potential rights are violated. To tease out the relationship between the private and government sectors, this article, for sake of argument, accepts as fact that surveillance is a core government function and that data is a public resource collected by private organizations.[35] While those assumptions may be challenged by different definitions of what constitutes a public function, public resource, or mode of collection, this article does not take on those challenges. It also does not ask the normative question of whether data collection should cease or the descriptive inquiry of whether data collection could even be halted if the public wanted it to be.[36]

31. *Id.* at 2490.

32. Lee Raine et al., *Anonymity, Privacy, and Security Online*, PEW RES. CTR. (Sept. 5, 2013), http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/.

33. *Id.*

34. Editorial, *A Second Front in the Privacy Wars*, N.Y. TIMES, Feb. 24, 2014, at A18. While technology and advertising industries have argued that an individual's self-regulation is the best mechanism for privacy, even the White House doubts whether social media companies "allow us to control and protect our privacy as the data is used and reused." EXEC. OFFICE OF THE PRESIDENT, *supra* note 4.

35. "Information is a public good in the strict economic sense, and is also input into its own production process." *See* Yochai Benkler, *The Political Economy of Commons,* 4 EUROPEAN J. FOR INFORMATICS PROF. 1, 7 (2003).

36. Heidegger questioned our orientation to technology and argued that our response to the various problems brought about by technology cannot be solved simply by making the technology better or simply "opting out." Thus, he argued, "we shall never experience our relationship to the essence of technology so long as we merely conceive and push forward the technological,

Rather, this article simply examines the structure surrounding data collection in terms of privatization, and asks whether certain legal doctrines may be triggered, including the Fourth Amendment. To do so, this article will first set out a definition of a privatization and use the military as an example. In Section II, the article will then engage in a short history of the Internet to show how electronic data collection was a core government function later "privatized" by Silicon Valley corporations. Section III will then explain how this dynamic between private and public oversight raises Fourth Amendment concerns. Finally, the Conclusion will then set out suggestions for the future, including a potential justification for new privacy rights.

A. *What Is Privatization?*[37]

The term "privatization" is most commonly used to refer to any shift of government activities from a public agency to the private sector. The difficulty in understanding this term is that throughout history, private organizations have often shared responsibilities with government, particularly when dealing with commerce.[38] In Greece, for instance, the government owned the land, forests, and mines, but contracted out the business of cultivating these resources to private hands.[39] This commercial realm created the traditional lines

put up with it, or evade it." *See* MARTIN HEIDEGGER, THE QUESTION CONCERNING TECHN. 4 (William Lovitt trans., Harper & Row 1977). But Heidegger went even further to state that technology should not be halted because it descriptively offers truth. *Id.* at 5. "Technology is therefore no mere means. Technology is a way of revealing. If we give heed to this, then another whole realm for the essence of technology will open itself up to us. It is the realm of revealing, i.e., of truth." *Id.* at 12.

37. While most people may have some familiarity with the term privatization, it is important to characterize this phenomenon and limit its scope with regard to this article.

38. *See* WILLIAM L. MEGGINSON, THE FINANCIAL ECONOMICS OF PRIVATIZATION 6 (2005).

39. In the Roman Republic, the "publicani" were a special sect of government contract workers who were relegated to the discrete task of fulfilling the state's economic requirements. This included private groups that built Roman streets and temples, managed public properties, and collected taxes, but it did not include the outsourcing of more fundamental government responsibilities like creating legislation or building an army. *Id.*

for government and private overlap.

But following both World Wars, under the leadership of the Prime Minister of the United Kingdom, Margaret Thatcher, the traditional boundary between private and public oversight began to slide beyond purely commercial tasks to other "core" or "inherent" functions of government, including postal services, utilities, transportation, school systems, prisons, and welfare.[40] This changing notion of responsibility began the public conversation of modern notions of privatization.

The term "privatization" was coined as late as 1969[41] by business scholar Peter Drucker. Drucker stated that during the 1940s, in the wake of both World Wars, nation-states had overextended themselves into the private realm in an effort to provide citizens with much-needed public services.[42] As the panacea to this problem, Drucker suggested "privatization" – a "systematic policy of using the other, the nongovernmental institutions of the society [i.e. private organizations], for the actual . . . performance"[43] of government function.[44] Drucker's idea was to eliminate government bureaucracy by having private organizations wield control.[45]

Soon thereafter, Thatcher found Drucker's term used in a pamphlet titled "A New Style of Government" and usurped it for her own project of mass deregulation and outsourcing of "core" government tasks.[46] In her privatization campaign,

40. *See* DANIEL YERGIN & JOSEPH STANISLAW, THE COMMANDING HEIGHTS: THE BATTLE BETWEEN GOVERNMENT AND THE MARKETPLACE THAT IS REMAKING THE MODERN WORLD (1998).

41. *See* German Bell, *The Coining of "Privatization" and Germany's National Socialist Party*, 20 J. ECON. PERSPECTIVES 187 (2006).

42. PETER F. DRUCKER, THE AGE OF DISCONTINUITY: GUIDELINES TO OUR CHANGING SOCIETY 229 (1969) ("It has no choice but to be 'bureaucratic.").

43. *Id.* at 234.

44. Conservative David Howell then used the term in a pamphlet titled "A New Style of Government," which Margaret Thatcher then picked up. YERGIN & STANISLAW, *supra* note 40.

45. *Id.*

46. Unlike "commercialization," where state-owned companies were supposed to begin acting like private companies, Thatcher had in mind something "much farther." For her and others, like British conservative Keith Joseph, "they had something far more radical and original in mind: They wanted to get the government out of business." YERGIN & STANISLAW, *supra* note 40, at 96.

Thatcher sold off over thirty government businesses,[47] and subsequently focused on outsourcing government schools, prisons, and welfare programs.

Thatcher's campaign quickly spread beyond the United Kingdom. On the other side of the Atlantic, President Ronald Reagan[48] froze more than 170 pending regulations on American business in the ten days following his inauguration.[49] He appointed George Bush, his eventual successor, to lead a deregulation task force, and instituted a commission on privatization.[50] In the decade after President Reagan's term, the turn toward a more private division of government continued.[51]

47. YERGIN & STANISLAW, *supra* note 40, at 114. In a speech given to the Fraser Institute, Thatcher described how the process fomented during her tenure:

> We had [forty-six] major industries in the hands of government, that is, they were nationalized. I took the view that governments don't know very much about running industry. The people who do know are the ones who are in it. What is more, it gives governments far too much power to have control over those industries, and it gives them far too much temptation, as when you want to make the appropriate changes or get rid of surplus labour and people would come streaming to their MP to ask for extra subsidies. That's not how you build a prosperous economy. So we had to privatize [forty-six] major industries. Most of them are now privatized.

Margaret Thatcher, *Speech to the Fraser Institute ("The New World Order")* (Nov. 8. 1993), http://www.margaretthatcher.org/document/108325.

48. "Margaret Thatcher was the forerunner who made Reagan possible. The 1979 campaign was the direct model from which we took much of the 1980 Republican campaign. Reagan drew great strength from Thatcher and her courage and toughness . . . ." Interview with Newt Gingrich (Spring 2001), *available at* http://www-tc.pbs.org/wgbh/commandingheights/shared/pdf/ufd_privatizethatcher_full.pdf.

49. *See* JAMES COOPER, MARGARET THATCHER AND RONALD REAGAN: A VERY POLITICAL SPECIAL RELATIONSHIP 145 (2012).

50. *See* Tom Raum, *Reagan, Thatcher Forged a Close, Lasting Bond,* THE BIG STORY (Apr. 9, 2013, 12:09 AM), http://bigstory.ap.org/article/reagan-thatcher-forged-close-lasting-bond.

51. In 1996, the Alaska Power Administration and the federal helium reserves were privatized. Just a year later, the Elk Hills Petroleum Reserve was sold for $3.7 billion. *Id.*

However, one of the more difficult areas to fully privatize was the realm of technology. Since its founding, American jurisprudence has required shared government and private oversight of technological innovation. For example, Article I, Section 8 of the U.S. Constitution states Congress is empowered "to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[52] The founding document also grants Congress the power to fix "the Standard of Weights and Measures," and to establish "Post Offices and Post Roads."[53]

As explained in more detail below, the Internet fell right into this category. At the height of the Cold War, in 1945, the government developed a defensive military strategy that involved government funding of technology and engineering to overcome new age warfare.[54] President Franklin D. Roosevelt had come to realize that just as "air power was the alternative to a large army, that technology, by corollary, was the alternative to manpower."[55] Vannevar Bush, President Roosevelt's trusted aid and a member of the Manhattan Project laid out this policy more concretely in his report titled, "Science: The Endless Frontier."[56] Bush advocated, "Our ability to overcome possible future enemies depends upon scientific advances which will proceed more rapidly with diffusion of knowledge than under a policy of continued restriction of knowledge now in our possession."[57]

While Roosevelt's Administration would not see the fruits of its labor, the implementation of Bush's policy[58] would

52. U.S. CONST. art. 1, § 8, cl. 8.

53. U.S. CONST. art. 1, § 8, cl. 5, 7. Similarly, James Madison proposed a national "University" to encourage "the advancement of useful knowledge and discoveries.

54. *See* JOHNNY RYAN, A HISTORY OF THE INTERNET AND THE DIGITAL FUTURE 18 (2010).

55. *Id.*

56. Vannevar Bush, *Science The Endless Frontier: A Report to the President by Vannevar Bush, Director of the Office of Scientific Research and Development* (July 1945), *available at*, https://www.nsf.gov/od/lpa/nsf50/vbush1945.htm

57. *Id.*

58. RYAN, *supra* note 54, at 11.

eventually give rise to the Internet.[59] But by the 1980s, government involvement would begin to taper off its involvement in technology. As Reagan privatized other government businesses, the federal government also began downsizing its role in overseeing the structure of the Internet and supported private corporations as they ventured to take it over.[60] "This began the ascendance of Silicon Valley over all other technology centers, with its more open, freewheeling start-up culture. . . . The center of gravity of innovation moved decisively from the behemoths of the post-war era to newer, more nimble competitors."[61]

Nevertheless, the governmental roots of the Internet were not entirely extirpated.[62] Like many other public functions where government has ceded control, government continued to have a vested interest in the organization and use of the Internet. Therefore, while privatization commonly means the actual divestiture of state-owned programs by private investors,[63] this article will employ a definition that applies where public functions are relegated to the nongovernmental sector but government continues to have a role in oversight.[64]

In such circumstances, "more is altered than mere

59. Jim Manzi, *The New American System,* NATIONAL AFFAIRS, Issue 19 (Spring 2014) ("From World War II through about 1975, th[e] public-private complex [on the Internet] was at the frontier of innovation, producing (among many other things) the fundamental components of the software industry, as well as the hardware on which it depended. Government agencies collaborated with university scientists to develop the electronic computer and the internet. The Labs invented the transistor, the C programming language, and the UNIX operating system.").

60. Similar, to the rise of the Internet in the 1940's, as Thomas Piety argues in his recent book, *Capital in the 21st Century,* it was during this same time period that the welfare state began to grow. Thomas Piety, CAPITAL IN THE 21ST CENTURY (2014). As argued later in this paper, the Internet was similarly privatized as was vast portions of the welfare state.

61. Manzi, *supra* note 59.

62. As discussed below, law enforcement continues to retain an active role in use of the Internet Paul Star, *The Meaning of Privatization*, 6 YALE L. POL'Y REV. 6 (1988).

63. Finally, the last common use involves government selecting a private entity to deliver a public service that had previously been produced in-house by public employees – also known as outsourcing. *Id.*

64. *See* Daphne Barak Erez, *Three Questions of Privatization, in* COMPARATIVE ADMIN. L. 493, 496 (Susan Rose-Ackerman & Peter L. Lindseth eds., 2010).

organizational arrangements to promote governmental economy."[65] The rights of citizens are potentially put at risk because the Constitution only restricts activities of the government not private entities. In order to understand the constitutional and normative problems that arise in these circumstances, this article will introduce an analogically similar situation where the United States government withdrew from one of its most crucial public functions: the military.

B. *What Is the Problem with Privatization of "Core" Government Functions: The Military and the Internet*

In his 2007 State of the Union Address, President George W. Bush made a plea:

> Tonight, I ask the Congress . . . to design and establish a volunteer civilian reserve corps. Such a corps would function much like our military reserve. It would ease the burden on the Armed Forces by allowing us to hire civilians with critical skills to serve on missions abroad when America needs them.[66]

Soon after, the executive branch came under increasingly sharp attack for its retreat from military responsibilities during the Iraq War.[67] In particular, the Administration was criticized for leaving its military responsibilities to private hands, namely to a group called Blackwater.[68]

Traditionally, the military has been deemed an inherent

65. Robert S. Gilmour and Laura S. Gensen, *Reinventing Government Accountability: Public Functions, Privatization, and the Meaning of State Action*, 58 PUB. ADMIN. REV. 247 (1998).

66. Pres. George W. Bush, *State of the Union*, Jan. 2007, http://www/whitehouse.gov/news/releases/2007/01/20070123-2.html

67. JEREMY SCAHILL, BLACKWATER: THE RISE OF THE WORLD'S MOST POWERFUL MERCENARY ARMY (2007); Robert Koulish, *Blackwater and the Privatization of Immigration Control*, 20 ST. THOMAS L. REV. 462 (2007).

68. *Id.*

function of government.[69] In particular, the actual strategy, armament, and implementation of warfare have been reserved for government oversight.[70] While mercenaries, in addition to private military companies, have a long American lineage,[71] public control over the armed forces has still been deemed not only an essential part of representative democracy, but a fundamental component of determining government accountability.[72]

But at the turn of the century, as America grew into a small industrial nation, some facets of the military, particularly those dealing with commerce or administrative decisions, were increasingly delegated outside the democratic process.[73] For example, in *Myers v. United States*, the Supreme Court held that department heads were able to make minor military decisions as the President's "alter ego."[74] Similarly, during World War II, private companies produced most of the military's weaponry, later infamously called the "military-industrial complex" by President Dwight D. Eisenhower.[75]

However, during the Iraq War, the executive branch broke even one step further from tradition, and turned over control of

69. Paul Verkhuil, *Public Law Limitations on Privatization of Government Functions*, 84 N.C. L. REV. 397 (2005).

70. Martha Minow, *Outsourcing Power: How Privatizing Military Efforts Challenges Accountability, Professionalism, Democracy*, 46 B.C. L. REV. 989 (2004).

71. During the Revolutionary War the Continental Army relied heavily on European mercenary officers.

72. PETER SINGER, CORPORATE WARRIORS: THE RISE OF THE PRIVATIZED MILITARY INDUSTRY 22-26 (2003).

73. *See* Morgan v. United States, 298 U.S. 468 (1936), *reh'g denied*, 304 U.S. 1 (1938); *see also* Elena Kagan, *Presidential Administration*, 114 HARV. L. REV. 2245 (2001). Dean Kagan's view that statutory delegations to subordinates should be interpreted as channeling, but not limiting presidential control has to be squared with the mixed statutory delegations where Congress clearly gives the President and his subordinates separate duties. *See* Kevin M. Stack, *The Statutory President*, 90 IOWA L. REV. 539 (2005).

74. Myers v. United States, 272 U.S. 52, 133 (1926).

75. Stemming back to the years of the Founding Fathers, the need for delegation of Presidential authority including military efforts were often acknowledged. *See* United States v. Page, 137 U.S. 673, 680 (1891) (holding that orders issued by the President would be "acknowledged" to be his – regardless of his actual input).

the actual armament of soldiers to private contractors.[76] The Bush Administration was castigated for giving companies like Blackwater responsibilities that went far beyond purely economic tasks. For example, just days after President Bush's 2007 State of the Union, it was revealed that the company had conducted interrogations, orchestrated security operatives, and engaged in primary military attacks.[77] A *Washington Post* article noted that in the years following the terrorist attacks of Sept. 11, 2001, 1,931 private companies had worked on programs related to military tasks in about 10,000 locations across the United States.[78] Other sources reported that up to 70% of the budget of United States intelligence was being spent on contractors.[79]

These facts raised immediate concerns with regard to government accountability, legality, and distribution of power. First, employment of mercenaries raised the concern that paid individuals would more easily switch from a defensive posture to an aggressive position and commit human rights violations, as was the case in Abu Ghraib.[80] Second, there was a concern

76. Minow, *supra* note 70.

77. Blackwater, which had about 1,000 contractors in Iraq, had 195 "escalation of force incidents" and in 163 of those cases, Blackwater guns fired first. Ben Van Heuvelen, *The Bush Administration's Ties to Blackwater*, Salon (Oct. 2, 2007, 4:08 PM), http://www.salon.com/2007/10/02/blackwater_bush/. *See also* Paul R. Verkhuil, *Outsourcing and the Duty of Government* 4 (Jacob Burns Inst. for Advanced Legal Studies, Working Paper No. 149, 2008).

78. Dana Priest & William M. Arkin, *A Hidden World, Growing Beyond Control*, WASH. POST (July 19, 2010, 4:50 PM), http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/1/.

79. Jose L. Gomez del Prado & UN Working Grp. on Mercenaries, *Beyond WikiLeaks: The Privatization of* War, TRUTHOUT (Dec. 25, 2010, 7:10 PM), http://truth-out.org/archive/component/k2/item/93553:beyond-wikileaks-the-privatization-of-war; Jose L. Gomez del Prado, *The Privatization of War: Mercenaries, Private Military and Security Companies (PMSC)*, GLOBAL RESEARCH (Nov. 8, 2010), http://www.globalresearch.ca/the-privatization-of-war-mercenaries-private-military-and-security-companies-pmsc/21826.

80. Nils Rosemann, *The Privatization of Human Rights Violations – Business' Impunity or Corporate Responsibility - The Case of Human Rights Abuses and Torture in Iraq*, 5 NON-ST. ACTORS & INT'L L. 77 (2005). Because of their concerns on the impact on human rights, the Working Group on mercenaries in its 2010 reports to the UN Human Rights Council and General Assembly recommended a legally binding instrument regulating and monitoring contractors at the national and international level. P. W. Singer,

whether government obligations existed in the realm of international humanitarian law, if private actors worked on behalf of government.[81] Third, there was the worry that private contracts created an even larger incentive for private industry to deploy more security measures.[82]

While admittedly different, similar concerns arise in terms of the Internet. As the government removed itself from the infrastructure and organization of the Internet, private industries took control creating a series of conflicts. Questions remain whether private companies consider their behavior injurious to users, whether the government's constitutional obligations apply where private companies control data collection, and finally, whether government or private industry will change this structure where their incentives align to maintain the status quo. Before engaging more with these questions, Section II will explain how this privatized structure resulted in the United States.

II. The Internet: Governmental Origins

In large part, the Internet was born out of a growing Cold War concern that sensitive government data was vulnerable to attack. By the late 1950s, the government had several highly-centralized computer systems that collected sensitive data for the Pentagon, Census Bureau, and other agencies.[83] Many government communications were sent over telephone wires that could be easily infiltrated and most other branches of

CORPORATE WARRIORS. THE RISE OF THE PRIVATIZED MILITARY INDUSTRY (2003); Peter W. Singer, *Outsourcing War*, available at http://www.Salon.com (posted April 16, 2004); Peter W. Singer, *War, Profits and the Vacuum of Law: Privatized Military Firms and International Law*, 42 COL. J. TRANSN'L L. 521, 532 (2004).

81. *Id.*

82. "In the councils of government," he said, "we must guard against the acquisition of unwarranted influence . . . . The potential for the disastrous rise of misplaced power exists and will persist. We must never let the weight of this combination endanger our liberties or democratic processes." Dwight D. Eisenhower, Farewell Address (Jan. 17, 1961) (transcript available in the Dwight D. Eisenhower Presidential Library and Museum).

83. GARY SHELLY AND JENNIFER CAMPBELL, DISCOVERING THE INTERNET 11 (2012) (existed to do "specific, mission-critical work for the Census Bureau, the Pentagon, and other government agencies.")

government were beginning to turn to some form of technology susceptible to intrusion.[84] So in 1957, when the Soviet Union launched Sputnik into orbit, waves of panic rushed through the Administration[85] that America's intelligence was not only lagging, but that it could be eliminated with push of a button.[86]

In response, the Department of Defense was charged to create the Defense Advanced Research Projects Agency (DARPA).[87] The agency's mission was to research and develop projects that would expand the frontiers of technology and science. More specifically, DARPA was established to create an indestructible information system for government.[88] In 1962, J.C.R. Licklider, formerly of the Massachusetts Institute of Technology, was appointed to the head of DARPA's computer research efforts. Licklider wrote a series of papers in which he imagined a "galactic network" of computers that could share information with one another.[89] In his paper titled "Man-Computer Symbiosis," Licklider wrote of "[a] network of [computers], connected to one another by wide-band communication lines [which provided] the functions of present-day libraries together with anticipated advances in information storage and retrieval."[90]

In 1969, Licklider's idea came to fruition. DARPA, renamed as ARPANET, delivered its first node-to-node communication sent from UCLA to Stanford on refrigerator-

84. *Id.*

85. JANET ABBATE, INVENTING THE INTERNET 36 (1999).

86. PELIN AKSOY AND LAURA DENARDIS, INFORMATION TECHNOLOGY IN THEORY 280 (2007) (The "hierarchical, centralized nature of communication systems such as the traditional telephone network made them more susceptible to severe" attack).

87. *Id.*

88. *Id.*

89. Licklider worked from memos written by Paul Baran, who was employed by the private corporation Research and Development Corporation ("RAND"). RAND was the private arm of DARPA, a United States think tank originally founded by General Henry H. Arnold to research long-range, future warfare but became privatized in order to gather private funds. *A Brief History of RAND Corporation*, RAND CORP., http://www.rand.org/about/history/a-brief-history-of-rand.html (last visited Dec. 4, 2014). RAND was also the organization that helped develop the doctrine of nuclear deterrence.

90. J. C. R. Licklider, *Man-Computer Symbiosis*, HFE-1 IRE TRANSACTIONS ON HUMAN FACTORS IN ELECTRONICS 4–11 (1960).

sized switches called Interface Message Processors (IMPs).[91] By December of that year the University of California Santa Barbara and the University of Utah joined ARPANET network, making these four government-funded connections the foundation of the global network known today as the Internet.[92]

Over the next two decades the system exponentially grew under government oversight. By 1980, thirteen research centers joined ARPANET, but all had to be government approved.[93] The United States National Science Foundation (NSF) also took over DARPA and the basic hardware of the Internet.[94] The NSF controlled the Transmission Control Protocol/Internet Protocol (TCP/IP), widely considered the foundational communication protocols of the Internet, still in use today.[95] From 1980 to 1990, little was done on the Internet without government permission.

In addition to public restrictions, commercial actors were altogether banned from the Internet. According to legislation, advertising for commercial purposes was not allowed, and sales over the network were prohibited.[96] The NSF had a strict policy against commercial users and only allowed a few academic institutions to enter into contract to use the TCP/IP system.[97] This protocol was especially visible in the 1996 Telecommunications Act, the first major federal regulation for the communications industry.[98] Over 1,000 pages long, the Act,

91. SHELLY, *supra* note 83.

92. *Id.*

93. *Id.*

94. The NSF is an independent federal agency with a mission to promote the progress of science; advance the national health, prosperity, and welfare; and secure the national defense. *See* 42 U.S.C. §§ 1861-1885 (2012); 20 U.S.C. §§ 3911-3922 (2012) (granting the NSF additional authority).

95. TCP/IP allows information packets to be transported across *different* networks, despite differences in bandwidth, delay, and error properties associated with different transport media (*e.g.*, telephone line, radio, satellite). TCP/IP concepts were translated into operative protocols under ARPA contracts. *See id.* Other interconnection protocols were also developed, but the NSF eventually chose TCP/IP as the primary protocol for the NSFNET and correspondingly for the Internet. *Id.*

96. Shane Greenstein, *Commercializing the Internet*, 18 IEEE MICRO 6-7 (1998).

97. *Id.*

98. LESLIE DAVID SIMON, NETPOLICY.COM: PUBLIC AGENDA FOR A DIGITAL WORLD 215 (2000).

which took years of lobbying by private corporations, only mentioned the Internet twice.[99]

But just ten years later, the Internet had become an open field of burgeoning private growth. Several factors, starting in the 1980s, helped establish the slow privatization of the system. First, the academic community, at that time, began to use two new networks, Usenet and BITNET, which opened the Internet to the entire academic community beyond those simply involved in science research.[100] Also, private computer use slowly became prevalent with the introduction of Apple II, Macintosh, and IBM PC computers.[101] Perhaps most important, in 1989, a more advanced network called "World Wide Web" was created by Tim Berners-Lee, one of the fathers of the Internet.[102] Intending to open the Internet to a wider audience, Lee created a system that could not only send, but also receive information.

As the access, audience, and structure of the Internet changed, the government also made a political decision to gradually cede its control over the Internet. In the late 1980s, the Department of Defense separated itself from the network of civilian Internet users, splitting ARPANET in two.[103] The resulting military network, later named MILNET, would be used for military purposes exclusively, and the remaining portion "would continue to bear the name ARPANET and still be used for research purposes."[104] In 1987, NSF followed and contracted out the management and the operation of the net backbone to Michigan Educational Research Information Triad (MERIT), MCI, and IBM, which would offer commercial access.[105] The consummate change occurred in 1992, when

99. The near silence of the "Internet" is especially meaningful to how little commercialization had been developed by then, considering the legislation was over 1,000 pages long and was the subject of several years of lobbying from major telecommunications organizations.

100. SHELLY, *supra* note 83, at 14.

101. *Id.*

102. Jonathan Owen, *25 Years of the World Wide Web: Tim Berners-Lee Explains How It All Began*, INDEP., Jan. 21, 2015.

103. National Academy of Engineering, REVOLUTION IN THE U.S. INFORMATION INFRASTRUCTURE, 16 (1995).

104. *Id.*

105. Rajiv C. Shah & Jay P. Kesan, *The Privatization of the Internet's Backbone Network* 51 J. OF BROAD. & ELEC. MEDIA 93 (2007).

Congress finally decided to change its statute and lift NSF's previous restriction on commercial activities.[106]

III. Silicon Valley Steps In

A. *Who Are Some of the Players?*

In just one decade, the Internet would grow from a tool of science and military defense to a major economic resource. By 2006, the Internet was open for business to a new group of prospectors, who believed in the libertarian traditions of free code, free speech, and free data.[107] As shown below, through two examples, many Internet companies were created with the goal to collect, organize, and store data that, in some ways, fulfilled the initial goals of the government's post-Sputnik program to safely collect and exchange information. But unlike earlier iterations of the Internet, commercial use and copulation of information was no longer restricted.

1. Google

In 1997, Larry Page and Sergey Brin met at Stanford and developed a new idea for organizing data on the Internet. They registered the name Google.com — a play on the word *googol* the mathematical term for the number "1" followed by 100 zeros.[108] Google "reflect[ed] Larry and Sergey's mission to

106. "[T]he NSF encouraged the local and regional networks to seek commercial, non-academic customers, [to] expand their facilities to serve them," and "[thus, to] exploit the resulting economies of scale to lower subscription costs for all." Brett Frischmann, *Privatization and Commercialization of the Internet Infrastructure: Rethinking Market Intervention into Government and Government Intervention into the Market*, 2 COLUM. SCI. & TECH. L. REV. 1, 17 (2001).

107. Jonathan Groves, *Remember 2006? How the Internet Has Changed in the Past Five* Years, CHANGING JOURNALISM BLOG (Aug. 15, 2011), http://grovesprof.wordpress.com/2011/08/15/remember-2006-how-the-internet-has-changed-in-the-past-five-years/.

108. *Our History in Depth*, GOOGLE,

organize a seemingly infinite amount of information on the web."[109] As explained in their proposal for the company, "Google is designed to scale well to extremely large data sets."[110] In essence, the two hoped to organize, but also keep diffuse the infinite amount of information on the Internet.

The idea stemmed from Page's doctoral work at Stanford where he first "found the Web interesting primarily for its mathematical characteristics."[111] Each computer was a node, and each link on a Web page was a connection between nodes — a classic graph structure," but one that had no ordering principles.[112] The desire was to make sense of the sprawling openness. As *Wired* magazine reported, while it "was Tim Berners-Lee's desire to improve this system that led him to create the World Wide Web . . . it was Larry Page and Sergey Brin's attempts to reverse engineer Berners-Lee's World Wide Web that led to Google."[113]

This "reverse engineering" was key to Google's economic success. The company would profit from knowing how to organize information, and more importantly, from learning how to collect even more data from users. The new data points would not only increase the efficacy of the company's algorithms, but also create a more complete collection of user profiles to sell to advertisers.[114] Google's data dossiers would become the lynchpin to the company's economic success, but also the main reason for conflicts with users concerned with privacy.

Most recently, these clashes came out in a class-action lawsuit filed against Google for its long-held practice of electronically scanning the contents of user's Gmail accounts to

https://www.google.com/about/company/history/ (last visited Dec. 4, 2014).

109. John Battelle, *The Birth of Google*, WIRED, Aug. 2005, no. 13.08, *available at* http://archive.wired.com/wired/archive/13.08/battelle.html?pg=1&topic=battelle&topic_set=.

110. Sergey Brin and Lawrence Page, *The Anatomy of a Large-Scale Hypertextual Web Search Engine* (1998), http://infolab.stanford.edu/~backrub/google.html

111. Battelle, *supra* note 109.

112. *Id.*

113. *Id.*

114. *Id.*

sell ads.[115] Filed in federal court, in May 2013, plaintiffs complained "Google actively seeks out, collects, and stores vast amount of behavioral information regarding internet users [all of which] directly correspond[s] to advertising revenues."[116] The complaint asserted that the company's searches violated California's privacy laws and federal wiretapping statutes. Google argued in response, "all users of email must necessarily expect their emails will be subject to automated processing."[117]

But United States District Judge Lucy Koh ruled otherwise. The Court denied defendant's motion to dismiss by ruling that Google's conduct could not be described as an "ordinary course of business."[118] The Court wrote "Google's interception of Plaintiffs' emails and subsequent use of the information to create user profiles or to provide targeted advertising advanced Google's business interests" is not ordinary.[119] "'[O]rdinary course of business' cannot be expanded to mean anything that interests a company."[120]

While Google faces this litigation and others like it, dealing with collection of data, the company continues to grow, with revenue of $15.42 billion and ad revenue that is projected to increase by more than $5 billion — more than the total ad revenue of Yahoo or Microsoft.[121] However, the company's data collecting model is not unique. Today, the most successful websites are those that collect vast amount of data on their users.

2. Facebook

115. *In re* Google Inc. Gmail Litig., Amended Complaint, May 16, 2013, *available at* http://www.consumerwatchdog.org/resources/gmailcomplaint051613.pdf.

116. *Id.*

117. Brayden Goyette, *Google: Email Users Can't Legitimately Expect Privacy When Emailing Someone On Gmail*, THE HUFFINGTONPOST.COM (Aug. 13, 2013), http://www.huffingtonpost.com/2013/08/13/gmail-privacy_n_3751971.html.

118. *In re* Google Inc. Gmail Litig., 13-md-02430, U.S. District Court, Northern District of California 13-MD-02430-LHK (N.D. Ca. Sept. 26, 2013).

119. *Id.*

120. *Id.*

121. David Streitfeld, *Earnings and Sales From Google Disappoint*, N.Y. TIMES, Apr. 17, 2014, at B1.

With more than 1 trillion page views each month, Facebook is the busiest site on the Internet.[122] The company's growth is largely dependent on data. As Facebook's analytics chief Ken Rudin stated, "Facebook could not be Facebook without Big Data technologies."[123] In fact, at its genesis, the young Mark Zuckerberg told *The Harvard Crimson* that he was inspired to build Facebook because he wished "to create a centralized Website" to view profile information.[124] For Zuckerberg, Facebook would be the single site through which people could locate one another around a university, and eventually the world. The idea was no doubt a success.

Much more than Google, Facebook has become *the* company with the most detailed data about its users. In a recent Pew Research survey, Facebook was named the dominant social-networking platform.[125] Some 71% of online adults are now Facebook users and 73% of all those ages between the ages of 12 and 17 are members.[126] With over 2.5 billion content items shared per day, including approximately 2.7 billion "likes" and 300 million photos per day,[127] Facebook has become of the largest data collector on the Internet of personal information.[128] It "boasts unparalleled reach."[129] "In English, that means it's likely the largest database of people ever built, and contains more personal data than any other source."[130]

122. Data Center Knowledge, *The Facebook Data Center FAQ* (accessed Jan. 31, 2015), http://www.datacenterknowledge.com/the-facebook-data-center-faq/

123. Steve Rosenbush, *Here's How Facebook Manages Big Data*, WALL ST. J., Oct. 13, 2013.

124. Claire Hoffman, *The Battle for Facebook*, ROLLING STONE, June 26, 2008, no. 1055.

125. Aaron Smith, *6 New Facts About Facebook*, PEW RES. CTR. (Feb. 3, 2014), http://www.pewresearch.org/fact-tank/2014/02/03/6-new-facts-about-facebook/.

126. *Id.*

127. Eliza Kem, *Facebook is Collecting Your Data – 500 Terabytes a Day*, GIGAOM (Aug. 22, 2012, 3:25 PM), http://gigaom.com/2012/08/22/facebook-is-collecting-your-data-500-terabytes-a-day/.

128. *See How Facebook Sells Your Personal Information*, DISCOVERY NEWS (Jan. 24, 2013, 2:26 PM), http://news.discovery.com/tech/gear-and-gadgets/how-facebook-sells-your-personal-information-130124.htm.

129. *Id.*

130. *Id.*

Initially, advertising had been anathema to the Facebook model. The company prided itself on being independent from advertisers. But in 2013, when stock prices began to plummet and financial stress hit, CEO Mark Zuckerberg suggested exploring ads in the site's News Feed.[131] Over the next several months, Zuckerberg grew to embrace the idea of "nonsocial ads," those that were not tied to users' likes.[132] Ad sales quickly rose 53% to $1.81 billion in the second quarter. It was the company's largest jump ever.[133] According to Adobe Systems Inc., this year, Facebook is forecast to profit significantly from its data; its ad revenue is projected to jump 50%.[134]

B. *Enabling Silicon Valley: Preference for Speech over Privacy*

The growing culture of data-collection is in large part enabled by a double-edged sword in the American legal system. While no comprehensive privacy regime exists in the United States, free speech is vigorously protected under the First Amendment. Therefore, almost any creation, collection, and distribution of information is encouraged, without any privacy limitation. Defamation law is a prime example. While European countries balance the interests between an individual's privacy and the public's interest in newsgathering, under American libel law there is no balancing. As Supreme Court Justice Robert H. Jackson famously wrote in *West Virginia State Board v. Barnette*, "If there is any fixed star in our constitutional constellation," it is the protection under the First Amendment.[135]

This idolization of the First Amendment as the alpha and omega has at times led to awkward or inconsistent results.[136]

131. Evelyn M. Rusli, *Profitable Learning Curve for Facebook CEO Mark Zuckerberg*, WALL ST. J. (Jan. 5, 2014, 11:00 PM), http://online.wsj.com/news/articles/SB10001424052702303640604579296452086218242.

132. *Id.*

133. *Id.*

134. David Streitfeld, *Earnings and Sales From Google Disappoint*, N.Y. TIMES, Apr. 17, 2014, at B1.

135. 319 U.S. 624, 642 (1943).

136. FREDERICK SCHAUER, AMERICAN EXCEPTIONALISM AND HUMAN

For example, some scholars have argued that the First Amendment has become a tool for corporations to "opportunistically"[137] assert "economic liberty" arguments to avoid federal regulations.[138] Under the "economic liberty" justification, corporations questionably equate financial actions as forms of expression that should be protected despite government regulations.[139] Similarly, as explained below, in the realm of data, this imbalance has permitted both the collection of increasingly private data, as well as compliance with government requests for such information.

1. Privacy

It is well known that there is no overarching privacy right granted within the Constitution. No Amendment explicitly protects privacy, and very few laws give any attention to it. In fact, the right to privacy is a very nascent concept. Only after 1890, when two Boston attorneys, Louis Brandeis and Samuel D. Warren published a brief on privacy, was the right even considered.[140] It took nearly a century after the brief was written, in 1964, for the Supreme Court to even recognize a privacy right existed. Since then, courts have often limited the

RIGHTS 29-56 (Michael Ignatieff ed., Princeton Univ. Press 2005) [hereinafter Schauer, AMERICAN EXCEPTIONALISM]; Frederick Schauer, *The First Amendment as Ideology*, 33 WM. & MARY L. REV. 853, 853-69 (1992) [hereinafter Schauer, *First Amendment as Ideology*].

137. Frederick Schauer, *First Amendment Opportunism* (John F. Kennedy Sch. of Gov't, Harv. Univ. Faculty Research, Working Paper No. 00-011) [hereinafter Schauer, *First Amendment Opportunism*], *available at* http://papers.ssrn.com/paper.taf?abstract_id=253832.

138. Victoria Baranetsky, Note, *The Economic- Liberty Approach of the First Amendment: A Story of American Booksellers v. Hudnut*, 47 HARV. C.R.-C.L. L. REV. 169 (2012).

139. Nat'l Ass'n of Mfrs. v. SEC, 748 F.3d 359 (D.C. Cir. 2014), *overruled by* Am. Meat Inst. V. U.S. Dep't of Agric., 760 F.3d 18 (D.C. Cir. 2014) (striking down the SEC's conflict minerals disclosure rule in part by holding the SEC rules violate the First Amendment by compelling companies to disclose in SEC filings and on their websites if any of their products have "not been found to be 'DRC conflict-free.'").

140. *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193 (1890) (arguing that American law ought to recognize and protect a right to privacy). Warren and Brandeis are often credited with inventing the concept. *See* Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 1 (1979).

protection to use in sex cases, and even in that context, largely undermined it.

For technology law, the lack of a privacy regime is an especially growing problem in terms of data collection. As privacy specialist, Ryan Calo writes in a recent article, if a user wishes to sue a social-media company for selling profile information to an advertiser[141] currently no privacy law exists to enforce against it.[142] To prove his point, Calo cites Instagram's actual privacy policy, which states:

> you hereby grant to Instagram a non-exclusive, fully paid and royalty-free, transferable, sub-licensable, worldwide license to use the Content that you post on or through the Service, subject to the Service's Privacy Policy [and] we may use information that we receive to . . . provide personalized content and information to you and others, which could include online ads or other forms of marketing.[143]

While some companies are changing their privacy policies, the fact remains that most companies rely on selling personal data whether users sign an agreement or not.[144]

Given the dearth of a privacy regime, many legal academics have begun to write on the subject in hopes of inspiring a broader constitutional protection.[145] In the

141. Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014).

142. *Id.*

143. *Id.* (citing *Privacy Policy*, INSTAGRAM (Jan. 19, 2013), http://instagram.com/legal/privacy/#).

144. *Id.*

145. *See* Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1132 (2011); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (2013); Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1468 (2000) ("Privacy-destroying technologies can be divided into two categories: those that facilitate the acquisition of raw data and those that allow one to process and collate that data in interesting ways."); Paul Schwartz, Commentary, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 820 (2000) ("The leading paradigm on the Internet and in the real, or off-line world, conceives of privacy as a personal right to control the use of one's data."); Lior Jacob Strahilevitz, *Toward A Positive Theory of Privacy Law*,

meantime, while no comprehensive federal requirement governs, a small number of federal statutes exist to handle the collection, storage, use, and disclosure of data. Notable examples include, the Health Insurance Portability and Accountability Act (protecting health care information), the Gramm-Leach-Bliley Act (information gathered by financial institutions), the Fair Creditor Reporting Act (credit-related information), and the Children's Online Privacy Protection Act (information pertaining to children). However, these statutes lack any comprehensive goal or structure.

In addition to these statutes, the Federal Trade Commission ("FTC") legislated by the Federal Trade Commission Act is the closest agency to maintain some policing power over privacy on the Internet.[146] The agency, established in 1914, is charged with two specific goals: to protect consumers from unfair or deceptive business practices, and to prevent anticompetitive policies.[147] In terms of protecting consumer privacy, the agency has been a longtime supporter of the Fair Information Practice Principles that form the foundation of a number of state and federal data privacy laws. The agency has also asserted privacy concerns more proactively in a variety of high-profile actions against Internet companies.

Most visibly, in 2011, the agency investigated whether Google and Facebook violated Section 5 of the FTC Act, which prohibits "unfair methods of competition."[148] According to the

126 HARV. L. REV. 2010, 2022-33 (2013) (analyzing the discriminatory effect of big data on some consumers). *See generally* ELI PARISER, THE FILTER BUBBLE: WHAT THE INTERNET IS HIDING FROM YOU (2011); JOSEPH TUROW, THE DAILY YOU: HOW THE NEW ADVERTISING INDUSTRY IS DEFINING YOUR IDENTITY AND YOUR WORTH (2010); JOSEPH TUROW, NICHE ENVY: MARKETING DISCRIMINATION IN THE DIGITAL AGE (2006).

146. The EU has long been keen on these issues. The EU's privacy regime takes a more uniform approach to the processing of data. In 1995, the European Union released the EU Data Protection Directive. As part of its implementation, each member state created a national enforcement agency known as the data protection authority, which tasked with enforcing the nation's privacy regulations. Under the EU privacy regime, all data must be processed in a manner that is fair, lawful, and legitimate; including protections for accuracy, a specific purpose, and use with the consent of the individual. These extreme rules long garnered a definite distaste in the Silicon Valley; and the Snowden revelations certainly did not help.

147. FTC, *About the FTC*, http://www.ftc.gov/about-ftc.

148. This undefined term has been interpreted by courts to give the FTC

FTC's complaint, Google misrepresented to users of Apple Inc.'s Safari Internet browser that it would not place tracking "cookies" or serve targeted ads to those users, violating an earlier privacy settlement between the company and the FTC.[149] Similarly, Facebook was said to have "deceived" its customers by "telling them they could keep their information on Facebook private and then repeatedly allowing it to be shared and made public."[150]

Ultimately, both companies faced consequences. Facebook settled the case. The agreement barred the company from making further misrepresentations about privacy settings[151] and also required the company to obtain consumers' affirmative express consent before enacting changes to their privacy preferences.[152] Google agreed to pay a record $22.5 million civil penalty to settle the charges and both companies are required to submit privacy audits until the year 2032.[153] "When companies make privacy pledges, they need to honor them," said Jon Leibowitz, Chairman of the FTC.[154]

"broad powers designed to enable it to cope with new threats to competition as they arise." E.I. du Pont de Nemours & Co. v. FTC, 729 F.2d 128, 137 (2d Cir. 1984).

149. *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, FED. TRADE COMM'N (Aug. 9, 2012), http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

150. *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*, FED. TRADE COMM'N (Nov. 29, 2011), http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

151. *Id.*

152. Frederic Lardinois, *Facebook And FTC Settle Privacy Charges — No Fine, But 20 Years of Privacy Audits*, TECHCRUNCH.COM (Aug. 10, 2012), http://techcrunch.com/2012/08/10/facebook-ftc-settlement-12/. The company was also prevented from accessing a user's material more than 30 days after the user has deleted his or her account.

153. *Privacy Practices in Google's Rollout of Its Buzz Social Network*, FED. TRADE COMM'N (Mar. 30, 2011), http://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.

154. According to the FTC complaint, Google launched its Buzz social network through its Gmail web-based email product and led Gmail users to believe that they could choose whether or not they wanted to join or leave the network, while the options were ineffective. "In response to the Buzz launch, Google received thousands of complaints from consumers who were concerned

While a holistic privacy regime still remains in progress, the recent FTC actions suggest a possible new turn for regulations, especially as Americans grow more concerned about their personal data. Still, the hope for working towards a culture of privacy is difficult to imagine, where little legal regime exists to support it, and especially given that the dueling protection for free speech is so vastly protected.

2. Freedom of Speech

In contrast to the privacy doctrine, free speech has had longstanding protection in the American legal structure. As the Supreme Court has written, this freedom is "the matrix, the indispensable condition of nearly every other form of freedom."[155] In fact, in First Amendment cases before the Supreme Court this past term, the party asserting free speech was more often than not the prevailing party. These odds are in large part due to the courts' expansion of protected categories of speech that were previously prohibited.[156] For example, in the 1970s, the Supreme Court granted protection to commercial speech, a category of speech previously not afforded full protection.[157] More recently, protected speech has also included corporate decisions as well as nondisclosures.[158]

Various companies have used this expanding protection to build competitive business structures.[159] For example, several airlines "employed the First Amendment to resist efforts to force them to list the full price of tickets."[160] Similarly, Google argued that the company's use of data is free speech and

about public disclosure of their email contacts which included, in some cases, ex-spouses, patients, students, employers, or competitors. According to the FTC complaint, Google made certain changes to the Buzz product in response to those complaints." *Id.*

155. Palko v. Conneticut, 302 U.S. 319 (1937)

156. Tim Wu, *The Right to Evade Regulation How corporations hijacked the First Amendment*, NEW REPUBLIC (June 3, 2013), http://www.newrepublic.com/article/113294/how-corporations-hijacked-first-amendment-evade-regulation.

157. *Id.*

158. *Id.*

159. *Id.*

160. *Id.*

enforcement of tort and antitrust laws is an impingement on those rights.[161] First Amendment scholars, Eugene Volokh and Donald Falk explained the theory in more depth in a white paper funded by Google.[162] The paper states that just like editorial judgments at a newspaper, Google's data use is only an arrangement of content.[163] Sections titled "The First Amendment Fully Protects Aggregation of Materials Authored by Others" and "The First Amendment Protects Search Engine Results Against Antitrust Law" further argued that the government's concerns, including privacy, are secondary to protecting "economic" speech.[164]

While some academics criticized the White Paper,[165] other companies quickly implemented the argument in litigation. For example, in 2007, when customers sued Verizon for secretly monitoring and distributing data to the federal government, in accordance with the Electronic Communications Privacy Act (ECPA), the company quickly employed Google's argument.[166] Under ECPA, magistrate judges are allowed to issue pen/trap orders which allow the

161. *Id.* However, there is precedent that content aggregators can face antitrust liability. For example, in *Turner Broadcasting System Inc. v. FCC*, 512 U.S. 622, 649 (1994), the Supreme Court wrote that unlike a cable operator, a newspaper does not possess the power to obstruct readers' access to other competing publications – suggesting that the First Amendment protections of a news agency cannot overcome all anticompetitive considerations and such.

162. Eugene Volokh and Donald M. Falk, *First Amendment Protection for Search Engine Search Results*, April 20, 2012 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2055364

163. *Id.* It makes this claim based on the converse being true, "[l]ikewise, the Ninth Circuit has concluded that even a newspaper that was plausibly alleged to have a 'substantial monopoly' could not be ordered to run a movie advertisement that it wanted to exclude, because '[a]ppellant has not convinced us that the courts or any other governmental agency should dictate the contents of a newspaper." Assoc. & Aldrich Co. Inc., v. Times Mirror Co., 440 F.2d 133, 135 (9th Cir. 1971).

164. This new justification of the First Amendment as a tool for economic power has been noted elsewhere. *See supra* note 95 and accompanying text.

165. Kurt Wimmer, *Google and the First Amendment*, MEDIA INST. (June 21, 2012), http://www.mediacompolicy.org/2012/06/articles/first-amendment/google-and-the-first-amendment/; Tim Wu, *Free Speech for Computers?*, N.Y. TIMES, June 19, 2013, at A29.

166. *HEPTING V. AT&T*, ELECTRONIC FRONTIER FOUND., *available at* https://www.eff.org/cases/hepting.

government to monitor incoming and outgoing telephone numbers and even related metadata.[167] Verizon defended its actions by asserting that the government's surveillance, as well as Verizon's collection and compliance, was protected speech.[168] It wrote: "Communicating such factual information to the government would be speech that is fully protected by the First Amendment" – despite any privacy concerns.[169]

Today, this same argument has the potential of being employed in the various high-profile lawsuits filed against the government in the wake of the Snowden leaks.[170] The pending suits challenge the NSA's two principal surveillance programs. The first program, authorized under Section 215 of the U.S.A. Patriot Act allows the government to obtain bulk phone records, including phone numbers, as well as the date, time, and duration of calls.[171] The second program, authorized under FISA Amendment Act (FISA) Section 702, permits warrantless surveillance programs, including PRISM.[172] Through PRISM the NSA is able to obtain personal data from companies, such as Verizon, Microsoft, Google, and Facebook.[173]

In these cases, sincere concerns about privacy arise. Ordinarily, the Fourth Amendment requires an individualized warrant before the government can engage in surveillance of private information. However, similar to ECPA, FISA creates an alternate process through which a judge can authorize

167. *A Guardian Guide to Your Metadata*, GUARDIAN (June 12, 2013), http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=0000000.

168. Ryan Singel, *Verizon: Suing Us for Turning Over Customer Call Records Violates Our Free Speech Rights*, WIRED (May 4, 2007, 3:59 AM), http://www.wired.com/2007/05/verizon_suing_u/.

169. *Id.*

170. *See* Jewel v. Nat'l Sec. Agency, 673 F.3d 902 (9th Cir. 2011); Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013); ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013); First Unitarian Church of L.A. v. Nat'l Sec. Agency, No. 13-CV-03287 (N.D. Cal. filed Jul. 16, 2013); Smith v. Obama, No. 13-CV-0257 (D. Idaho 2013). The *First Unitarian* and *ACLU* complaints concern only telephone metadata, while the *Jewel* and *Klayman* suits target the Prism program as well.

171. 50 U.S.C. § 1861(b)(2)(A) (2012).

172. 50 U.S.C. § 1881a.

173. Glenn Greenwald and Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 7, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

sweeping surveillance programs without some further justification for monitoring. In *Klayman v. Obama*, the district court recognized that the government's bulk collection of metadata likely constitutes an unconstitutional search under the Fourth Amendment.[174] Judge Richard J. Leon wrote, "[b]ecause the Government can use daily metadata collection to engage in repetitive, surreptitious surveillance of a citizen's private goings on, the NSA database implicates the Fourth Amendment each time a government official monitors it."[175]

Given the similarity of these facts to the Verizon case, an increasing tension between the right to privacy and the right to free speech becomes apparent. While government surveillance of data potentially violates the Fourth Amendment, collection of that data is also arguably protected under the First Amendment. The tension between these fundamental rights has yet to be resolved but, as seen in the case of *Blackwater*, the question remains whether some privacy protections can be afforded to individuals, especially if private companies are providing a core government function, namely data collection?[176]

IV. Conclusion: Data Privacy and the *New* New Property?

Even before the changing winds of Edward Snowden and the NSA, the prevailing norm among the American public was that Internet users were responsible for keeping their own data

174. *Klayman*, 957 F. Supp. 2d at 41.

175. *Id*. However, while the government's potential Fourth Amendment violation raises one concern, there exists a similar but less discussed separate concern: that a corporations' right to collection of private data (ostensibly protected under the First Amendment) may perhaps circumvent the Fourth Amendment violations under FISA. In essence, is the First Amendment trumping the Fourth?

176. The European Union suggested controversial measures this year to protect its 250 million Internet users from online surveillance following the revelations that companies had aided the United States National Security Agency and other intelligence agencies, including in Europe to spy. The new rules would give people more protections as to who would be able to get access to their data and other privacy safeguards, including granting the individuals the right to be forgotten, or the ability for individuals the ability to erase data. David Jolly, *The European Union Takes Steps Toward Protecting Data*, N.Y. TIMES, March 13, 2014, at B2.

private.[177] Information placed on the Internet was assumed to be vulnerable to access, i.e. you post it, you lost it.[178] For instance, in 2010, after Facebook controversially loosened their privacy settings to make user's default sharing "Public," founder Mark Zuckerberg told the press that people no longer had an expectation of privacy.[179] "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people," he said.[180] "That social norm is just something that has evolved over time."[181] In fact, a survey conducted just days before the NSA news broke found that 85% of Americans already believed their

177. *See generally* Mary Madden, Pew Research Internet Project, *Privacy Management on Social Media Sites* (Feb. 24, 2012), http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/; danah boyd, *The Future of Privacy: How Privacy Norms Can Inform Regulation*, 32nd International Conference of Data Protection and Privacy Commissioners (October 29, 2010), http://www.danah.org/papers/talks/2010/PrivacyGenerations.html.

178. William A. Herbert, *No Direction Home: Will the Law Keep Pace with*

Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?, 2 I/S: J.L. & POL'Y INFO. SOC'Y 409, 409 (2006) (Technology "expands the means for privacy intrusions, thereby limiting the personal secrets and confidences that can be concealed . . .[n]ew technological tools diminish the ability of individuals to maintain a protected zone against physical, sensational, informational, and cyber intrusions."); Cristen Conger, *Is the Internet Destroying Privacy*?, DISCOVERY NEWS (Mar. 22, 2011), http://news.discovery.com/tech/is-the-internet-destroyingprivacy.html ("[i]t may be that social norms just haven't completely developed yet, but we end up revealing so much more than we likely would have without the Internet, and we reveal it to a much wider range of people"); *Facebook & Your Privacy: Who Sees the Data You Share on the Biggest Social Network*?, CONSUMER REPORTS (June 2012), http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm.

179. Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 10, 2010), http://www.theguardian.com/technology/2010/jan/11/facebook-privacy. Following Facebook, Twitter followed making public Tweets the default setting. *About Public and Private Tweets*, TWITTER, http://support.twitter.com/ articles/14016-about-public-and-protected-tweets (last visited Nov. 26, 2012).

180. *Id.*

181. *Id. See also* Irina Raicu, Markkula, *Are Attitudes About Privacy Changing?*, Center for Applied Ethics, Santa Clara Univ., http://www.scu.edu/ethics-center/privacy/attitudes/ (last visited Mar. 8, 2014).

online activity was being monitored.[182]

However, since the leaks, there is a growing public perception that users have no command over what they share. In a Pew Research Poll, conducted in November 2014, 91% of adults in the survey reported that they "agree" or "strongly agree" that consumers have lost all control over their information."[183] "Across the board, there is a universal lack of confidence" particularly because users no longer understand *how* or *what* information is collected.[184] Data no longer just refers to information collected from posts. It now includes information gathered from initial sign-up questions, metadata, and cross-referencing.[185] Since social media sites have become so deeply embedded in our social world[186] users can no longer protect their privacy by simply refraining to post information.[187] In this system, you log on, you lost it.

In addition, there is a growing perception among industry members and the government that Internet users function in an environment that unjustly requires them to relinquish privacy rights. Companies have recognized this increasing concern and responded with actions that suggest they have some obligation to their users to obtain consent or, at the very least, to inform their users of privacy policies.[188] For example,

182. Heather Kelly, *Some Shrug at NSA Snooping: Privacy's Already Dead*, CNN.COM (Jun 10, 2013), http://www.cnn.com/2013/06/07/tech/web/nsa-internet-privacy/.

183. Madden, *supra* note 177.

184. *Id.*

185. *A Guardian Guide to your Metadata*, GUARDIAN (June 12, 2013), http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance.

186. JOHN PALFRY AND URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 13, 19-20 (2010).

187. Madden, *supra* note 177.

188. *See* Farhad Manjoo, *Another Tech Company Finds the F.T.C. Looking Over Its Shoulder*, N.Y. TIMES (May 8, 2014), http://bits.blogs.nytimes.com/2014/05/08/will-a-government-settlement-improve-snapchats-privacy-dont-count-on-it/?_r=0; Issie Lapowsky, *Facebook Rolls Out Clearer Privacy Policy, But You Still Can't Control Your Data*, WIRED (Nov. 13, 2014). http://www.slate.com/blogs/moneybox/2014/11/28/uber_josh_mohrer_new_york_s_general_manager_is_facing_disciplinary_action.html; Alison Griswold, *Uber Takes "Disciplinary Actions" Against Its Top New York Manager Over Privacy Violations*, MONEYBOX.COM (Nov. 28, 2014), http://www.wired.com/2014/11/facebook-revamps-privacy-policy/.

in 2014, Facebook reversed some of its previous changes to its privacy settings from four years earlier and switched the default posting status from "Public" to "Friends only" for new users.[189] The Supreme Court has even suggested that the Fourth Amendment should protect information collected by mobile applications.[190] Internationally, the European Union has provided an even stronger protection of privacy.[191]

At the same time, the structure inducing this environment and providing outlets for data is largely funded and orchestrated by private organizations and law enforcement that both benefit from data collection. While companies profit from the sale of information about their users,[192] government is increasingly able to obtain information about its citizens for surveillance without following Fourth Amendment requirements. Although the increase in data creation and collection may not be an inherent wrong, where both government and private entities are incentivized to collect increasingly private information, without any check, some protections may be lacking.

In many ways the present circumstances, are similar to those addressed in Charles Reich's visionary 1964 article, "The New Property," which paved the groundwork for the due process revolution of twentieth century.[193] In his article, Reich argued that government largesse had become so invasive and unavoidable to private individuals that some forms of public assistance, like welfare, had become inevitable.[194] Where citizens are immediately divested of certain independences

189. Charlie Warzel, *Facebook Makes A Major Change To Its Privacy Policies*, BUZZFEED (May 22, 2014), http://www.buzzfeed.com/charliewarzel/facebook-makes-a-huge-change-to-its-privacy-policies#.wd6ogxwa5.

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

191. Jolly, *supra* note 176.

192. For example, Facebook's advertising guidelines state "the best ads are those that are tailored to individuals based on how they and their friends interact and affiliate with the brands, artists, and businesses they care about." Facebook Advertising Guidelines, FACEBOOK, http://www.facebook.com/ ad_guidelines.php (last revised Feb. 10, 2014).

193. Charles Reich, *Individual Rights and Social Welfare: The Emerging Legal Issues*, 74 YALE L. J. 1245 (1965).

194. *Id.* at 1255.

some entitlements are necessary, Reich argued.[195] He further analogized that traditional property rights afforded to real property owners should similarly be offered to these "new property" rights holders.[196]

The Supreme Court in its 1970 decision *Goldberg v. Kelly* adopted Reich's revolutionary framework.[197] In that case, New York State had denied twenty individuals their welfare benefits without first providing an adversarial hearing.[198] The Court held that a hearing was a procedural due process right required under the Fourteenth Amendment.[199] Justice William Brennan, writing for the majority, explained that members of society had come to depend on the need of government assistance and that "it may be realistic today to regard welfare entitlements as more like 'property' than 'gratuity'."[200] In later years, *Goldberg* was extended to other circumstances, including Medicaid,[201] food stamps,[202] and supplemental security income,[203] among others.

A potentially similar question exists today in the realm of the Internet and whether its structure of data creation and collection perhaps requires some further entitlements. Recognizing that social media sites on the Internet have become so entangled in our lives — so great and interstitial — and that the government depends on this structure to fulfill one of its fundamental functions seems to suggest that certain rights might flow from this dynamic – as was the case with new property rights.

However, as in the *Goldberg* line of cases, an important question remains whether protections arise even where private entities provide the service. In other words, one legal hurdle, in this area of law arises when private control interrupts "state action." Under the U.S. Constitution, civil liberties protected

195. *Id.* at 1254.
196. *Id.* at 1253.
197. Goldberg v. Kelly, 397 U.S. 254 (1970).
198. *Id.* at 255.
199. *Id.* at 274.
200. *Id.*
201. 42 U.S.C. § 1396 (2012).
202. 7 U.S.C. § 2020(e)(10) (2012).
203. 42 USC § 1383 (2012).

under the first ten Amendments, apply only where state officials have acted upon the individual. In contrast, private corporations, in general, do not have the same legal obligations to protect individuals. Given this rule, during the privatization of the 1980s, a question arose whether *Goldberg* protections applied where a private corporation provided the public service.

This question crystallized in the case of *Rendell-Baker v. Kohn*.[204] In *Rendell-Baker*, a privately run, but publicly-funded school fired a counselor hired under a federal grant.[205] There, the Court decided that no state action occurred because the private school did not act under state law when firing.[206] *Rendell-Baker* now stands for the proposition that when a private entity takes over a public function, the property interest is no longer protected. However, exceptions exist. In other cases, courts have held that state action is found when a private corporation provides a "public function."[207] Additionally, when private corporations are heavily regulated by the state, obligations may also exist.[208]

Today, an analogy can possibly be extended to provide rights with respect to data collected on the Internet. While private companies may control the initial organization and collection of data, a strong argument exists that ultimately data collection is a public function (especially when government eventually uses it for law enforcement purposes). In fact, as stated by the White House, in a recent report – electronic data is considered a public resource.[209] Similarly, there is a separate argument that state action also applies if

204. 457 U.S. 830 (1982).

205. *Id.* at 830.

206. *Id.* at 850.

207. Marsh v. Alabama, 326 U.S. 501, 506 (1946) (company town); *see also* Evans v. Newton, 382 U.S. 296, 299 (1966) ("That is to say, when private individuals or groups are endowed by the State with powers or functions governmental in nature, they become agencies or instrumentalities of the State and are subject to constitutional limitations."); Terry v. Adams, 345 U.S. 461 (1953).

208. *But see* Jackson v. Metro. Edison Co., 419 U.S. 345, 350-51 (1974) ("heavily regulated" electric utility is not a state actor); Moose Lodge No. 107 v. Irvis, 407 U.S. 163 (1972) (no state action in private club that held a state liquor license, despite the state regulation that accompanied the liquor license).

209. EXEC. OFFICE OF THE PRESIDENT, *supra* note 4.

government regulates these companies, perhaps in the form of the FTC.

The question of whether state action should apply is perhaps best illustrated in the context of telephone networks, such as Skype/Microsoft and Verizon. As early as 1878, the Supreme Court recognized an elevated privacy right in the content of communications.[210] In that case, the Court ruled that searching the content of a letter was unreasonable.[211] Nearly a century later, in *Katz v. United States*, the Court extended that protection to the content of individual's telephone calls by stating a person is "entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[212]

Today, that same Fourth Amendment protection is thought to apply to similar communications – such as those that take place on Skype even if a private company like Microsoft runs the program because the government's involvement is so entangled.[213] In fact, when Microsoft complied with the NSA's tapping of Skype chats, the company issued a memo, in which it stated that it had acted according to the government's directive and that it intended to continue its mutually supportive relationship with the government when moving forward.[214] While Microsoft's compliance is of intrigue – the separate question of whether these private/government actions violate some potential new rights. In essence, given the historical involvement of government on the Internet and the continued use of data by law enforcement a question remains

210. *Ex parte* Jackson, 96 U.S. 727 (1877).

211. *Id.*

212. Katz v. United States, 389 U.S. 347, 352 (1967).

213. *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1018-22 (2010) (comparing email content to the inside of a person's home, which also gets heightened Fourth Amendment protection); *see also* Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007) (finding people have a reasonable expectation of privacy in email content because it is material that the author "seeks to preserve as private") (internal quotation omitted), *vacated on other grounds* Warshak v. United States, 532 F.3d 521 (6th Cir. 2008).

214. *Responding to Government Legal Demands for Customer Data*, MICROSOFT (Jul. 16, 2013), http://blogs.microsoft.com/on-the-issues/2013/07/16/responding-to-government-legal-demands-for-customer-data/.

whether state action applies. Does government merely cede its surveillance and law enforcement responsibilities to private companies? Or under the rule of *Rendell-Baker* are those actions outside the zone of the state?

In any event, the circumstances with privacy on the Internet are in a period of flux. Many who helped create this structure have demanded some new protections. For example, Tim Berners Lee, told *The Guardian*, on the 25th anniversary after first drafting the World Wide Web, "We need a global constitution - a bill of rights." [215] Lee stated that his "open and neutral" creation had been taken advantage of by governments and corporate influences and that a new set of rules are needed to protect its mission,[216] including principles of privacy.[217] Perhaps the next question to ask is whether we need new property to provide those protections.

215. Jemima Kiss, *An Online Magna Carta: Berners-Lee Calls for Bill of Rights for Web*, GUARDIAN (Mar. 11, 2004), http://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web.

216. *Id.*

217. *Id.*