Maryland Law Review

Volume 76 | Issue 4 Article 6

Reviving the Public Trustee Concept and Applying It to Information Privacy Policy

Priscilla M. Regan

REVIVING THE PUBLIC TRUSTEE CONCEPT AND APPLYING IT TO INFORMATION PRIVACY POLICY

PRISCILLA M. REGAN*

INTRODUCTION

Three policy narratives in the 1980s and 1990s largely determined the path that information privacy policy would take. The first was the dominance of the individual rights definition of the problem of information privacy. Second was the Reagan administration's deregulation perspective, which was followed by the Federal Communications Commission ("FCC") stepping back from regulation in the "public interest, convenience and necessity." And third was the Clinton administration's admonition not to stifle innovation as the Internet developed. All three of these narratives are being challenged by events in the early part of the twenty-first century. The view that privacy is not only an individual right, but also a right that is important to society as a whole, has received more support in policy, philosophical, and legal literatures—and has called into question the effectiveness and relevance of policy based on the Fair Information Principles ("FIPs"). At the same time, the deregulatory policies of the Reagan administration have largely evolved into new forms of concentration in a number of industries—including those in the information and communication sectors—and have raised questions as to whether some of these companies have achieved the status of providing necessary or essential services and thus should be regulated. Finally, there is now a question of whether those who benefitted from the earlier era of free rein are now hampering Internet innovation by operating to stifle, or buy-up, new startups.

The quest in this Essay is inspired, in large part, by Ithiel de Sola Pool's 1983 analysis of the convergence of communications technologies, which had heretofore been regulated under three distinct regimes of print, common

*Dr. Regan is a Professor at the Schar School of Policy and Government at George Mason University. Prior to that, she was a Senior Analyst in the Congressional Office of Technology Assessment (1984-1989). From 2005 to 2007, she served as a Program Officer for the Science, Technology and Society Program at the National Science Foundation. Since the mid-1970s, Dr. Regan's primary research interests have focused on both the analysis of the social, policy, and legal implications of organizational use of new information and communications technologies. She was a member of the National Academy of Sciences, Computer Science and Telecommunications Board, Committee on Authentication Technologies and their Privacy Implications. Dr. Regan received her PhD in Government from Cornell University and her BA from Mount Holyoke College.

carriage, and broadcasting. De Sola Pool's analysis raises the question of what regime should provide the framework for communications policy of the future, particularly as applied to Internet communications. For Pool,

> The outcome to be feared is that communications in the future may be unnecessarily regulated under the unfree tradition of law that has been applied so far to the electronic media. The clash between the print, common carrier, and broadcast models is likely to be a vehement communications policy issue in the next decades. Convergence of modes is upsetting the trifurcated system developed over the past two hundred years, and questions that had seemed to be settled centuries ago are being reopened, unfortunately sometimes not in a libertarian way.[1]

Pool's primary concern was that speech remain free and unfettered from regulation in the new electronic era, as was truest under the print regime. Arguably, speech has remained generally free on the Internet and in electronic communications, as demonstrated by the Supreme Court's holding that the provisions of the Communications Decency Act designed to censor Internet material violated the First Amendment freedom of speech.[2] And, arguably, commercial speech has been somewhat privileged, especially online advertisements and targeted messages to consumers—with the effect that the privacy of consumers has been compromised. Although the conflict between free speech and privacy is not the focus of my analysis, it is instructive to note that this perceived conflict established an early line of policy discourse and provided legal, and even constitutional, rationales against strong information privacy policy and, in effect, may have closed off a path to a different approach to information privacy protection.[3]

---

1. ITHIEL DE SOLA POOL, TECHNOLOGIES OF FREEDOM 7–8 (1983).

2. *See, e.g.*, Reno v. ACLU, 521 U.S. 844, 864–85 (1997); Ira Glasser, *The Struggle for a New Paradigm: Protecting Free Speech and Privacy in the Virtual World of Cyberspace*, 23 NOVA L. REV. 627, 646 (1999).

3. Eugene Volokh voiced the concern that information privacy protections would endanger free speech by restricting the ability of others to communicate information about us and that free speech was the higher value to protect. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049, 1123–24 (2000). Both Paul Schwartz and Julie Cohen provided important and insightful responses to Volokh's analysis. Schwartz emphasizes that FIPs that require non-disclosure of information "help maintain the boundary between public discourse and the other realms of communication" and "safeguard deliberative democracy by shaping the terms of individual participation in social and political life." Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559, 1563–64 (2000). Cohen, in turn, argues, "[i]n the sense that counts for First Amendment purposes, personally-identified data is not collected, used or sold for its expressive content at all; it is a tool for processing people, not a vehicle for injecting communication into the 'marketplace of ideas.'" Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1414 (2000) (citing Dan L. Burk, *Patenting Speech*, 79 TEX. L. REV. 99 (2000)).

This Essay proceeds in four parts: First, this Essay provides a brief review of information privacy policy and practices and their relevance and effectiveness in today's information environment (such as big data, the Internet of Things, individual convenience compromising public convenience). Second, the Essay analyzes communications deregulation to identify key principles and to determine whether these are relevant to today's environment. Third, this Essay examines the current status of the Internet landscape; and fourth, provides a preliminary investigation of whether and how the public trustee concept might be applied to information privacy policy.

I. INFORMATION PRIVACY POLICY AND PRACTICES

The shortcomings of the current approach to information privacy law in the United States are generally and broadly recognized.[4] The current model, based on the FIPs, places the burden on individuals to monitor organizations in order to ensure that their information is accurate, complete, and used only for the purposes to which the individual has agreed. Although organizations are to give notice of their practices, such notice is often in the form of long, lawyerly statements that few read in either online or offline forms.[5] Updating or replacing FIPs has received renewed attention as information practices move from individual records to big data analytics. Additionally, there is increased recognition that privacy is not just important to the individual but

4. *See, e.g.*, Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 SOFTWARE L.J. 199 (1993); Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815 (2000); Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013); Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033 (1999).

5. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Notices*, 4 ISJLP 543 (2008). In their research, McDonald and Cranor found that the national opportunity cost for the time to read privacy policies is in the order of $781 billion, or seventy-six work days a year, given that the average American encounters almost 1,500 privacy notices a year. *See id.* at 552–65; Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, ATLANTIC (Mar. 1, 2012), http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

also is important to society more generally[6] and takes on some of the characteristics of a public good.[7]

The modern personal information economy has revealed the weaknesses of looking at privacy as a private good, or individual value, for which isolated individuals can bargain and negotiate to obtain the level of privacy protection that they desire. Instead, the information asymmetries of the personal information market, as well as the actions of other individuals, render it impossible for individuals either to procure reliable and complete information on the implications of revealing their information or to ensure that the actions of others will not implicate their privacy. On social networking sites, one's own privacy is dependent upon one's friends, friends of friends, professional colleagues, affinity sets, and others who have access to that individual's personal information. The actions of one person affect the privacy of others in that group.[8] The other way in which users expose data about one another is more complicated and less directly attributable to the actions of others with whom one actually interacts.[9] This is the landscape of big data where "individuals cannot know what the data they reveal means when aggregated with billions of other data points."[10] Ira Rubinstein notes that the information extracted from big data "is not only unintuitive and unpredictable, but also results from a fairly opaque process."[11]

Recently, a number of scholars have begun rethinking how the current status of personal privacy might best be conceptualized in a way that moves

6. Chapter 8 of my 1995 book, *Legislating Privacy*, set out one of the earliest arguments for the social importance of privacy and suggested three bases for its social importance: privacy's common value, its public value and its collective value. PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 213 (1995). A number of scholars have also recognized and further developed the social importance of privacy: Valerie Steeves, Helen Nissenbaum, Paul Schwartz, Beate Roessler, Paul Ohm, Daniel Solove. For the most recent writing on this, see SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES (Beate Roessler & Dorota Mokrosinska eds., 2015).

7. *See* Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385 (2015); *see also* Dennis D. Hirsch, *Privacy, Public Goods, and the Tragedy of the Trust Commons: A Response to Professors Fairfield and Engel*, 65 DUKE L.J. ONLINE 67 (2016); Priscilla M. Regan, *Response to* Privacy as a Public Good, 65 DUKE L.J. ONLINE 51 (2016).

8. Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 ISJLP 425, 428–29 (2011).

9. *See also* Solon Barocas & Helen Nissenbaum, *Big Data's End Run Around Anonymity and Consent*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 44 (Julia Lane et al. eds., 2014); Paul Ohm, *Changing the Rules: General Principles for Data Use and Analysis*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 96 (Julia Lane et al. eds., 2014); Priscilla M. Regan, *Big Data and Privacy*, *in* ANALYTICS, POLICY AND GOVERNANCE 204 (Jennifer Bachner et al. eds., 2017).

10. Fairfield & Engel, *supra* note 7, at 390.

11. Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INT'L DATA PRIVACY L. 74, 76 (2013).

beyond the individual rights and FIPs approach. A central component of this rethinking is to realistically examine the economics or market context in which personal privacy is negotiated, which logically and inevitably draws attention to the market failures, making it difficult, if not impossible, for individuals to protect their own privacy.[12] These market failures include, for example, the asymmetries in information about the flows of personal information, lack of transparency regarding data exchanges, and lack of knowledge about short-term and long-term implications and costs to the individual. The existence of such market failures, joined with the recognition of a social or public value of privacy, justifies thinking about privacy as a public good.

Scholars are currently pursuing at least four lines of analysis to conceptualize privacy as containing a collective or public good value and a different approach to protecting privacy. The first is to stress the negative externalities that result from the way that personal information is currently collected, used, and exchanged, and thus, explore how the tools and practices of environmental protection might be incorporated into personal information protection.[13] The second is to view the personal information landscape as experiencing a "tragedy of the commons." I have argued elsewhere that personal information can be viewed as a "common-pool resource,"[14] whose value to any one user is curtailed by other users because the common pool resource system is *overloaded* in that the collection of more personal information drives up the costs to both data subjects and users; *polluted* in that inaccurate, irrelevant, and out-of-date information contaminates the resource pools; and *over-harvested* in that more users take similar pieces of information from the pool, reducing the unique value of that information for any one user.[15] Somewhat similarly, the third way of conceptualizing a public good value of privacy is to draw attention to how the personal information landscape has resulted in the "tragedy of the trust commons."[16] Finally, the fourth is to use tools and analysis from behavioral and experimental economics to identify the negative externalities or spillovers

12. *See, e.g.*, Fairfield & Engel, *supra* note 7; A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. ILL. L. REV. 1713; Hirsch, *supra* note 7; Regan, *supra* note 7.

13. Froomkin, *supra* note 12; Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 7 (2006).

14. *See* ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION 30 (1990).

15. Priscilla M. Regan, *Privacy as a Common Good in the Digital World*, 5 INFO. COMM. & SOC'Y 382, 400 (2002).

16. Hirsch, *supra* note 13, at 29–30.

that individuals create in their own actions and to empower groups to protect privacy.[17]

Given the weaknesses of the current regulatory or, more accurately, self-regulatory, approach and the increasing appreciation for privacy's social importance, serious thinking about an appropriate public policy approach that recognizes the broad social value of information privacy is needed. I propose that the old model of public trustee, as applied, for example, to Ma Bell in the Communications Act of 1934 and as found in notions of fiduciary responsibility, is likely to be relevant again in today's personal information environment with large, concentrated firms providing multifaceted and interlocking services for individuals and organizations.

II. LOGIC OF COMMUNICATIONS AND TELECOMMUNICATIONS REGULATION AND DEREGULATION

Although a detailed review and analysis of the history of communications and telecommunications policy is far beyond the scope of this Essay, it is instructive to consider the traditional principles that guided policy in this area—and the logic for changing those principles in the mid-1980s. Such a review will reveal whether and, if so, which principles may be relevant in today's Internet environment.

From the Radio Act of 1927 until the deregulatory wave of the 1980s, broadcasting regulation under both the Federal Radio Commission ("FRC") and the FCC was based on the standard of the "public interest, convenience, and necessity."[18] Although the vagueness of this standard was recognized at the time, the general idea was to establish the fundamental principle that would help guide the development of the industry in an area where technology was likely to change and evolve.[19] As an author of the Radio Act of 1927 stated at the time:

> [I]n the present state of scientific development . . . licenses should be issued only to those stations whose operation would render a benefit to the public, are necessary in the public interest, or would contribute to the development of the art. . . . [T]he broadcasting

17. Fairfield & Engel, *supra* note 7.

18. *See generally* Glen O. Robinson, *The Federal Communications Act: An Essay on Origins and Regulatory Purpose*, *in* A LEGISLATIVE HISTORY OF THE COMMUNICATIONS ACT OF 1934, at 3, 14 (Max D. Paglin ed., 1989).

19. *Id.* at 18.

> privilege will not be a right of selfishness. It will rest upon an assurance of public interest to be served.[20]

The Act borrowed from the public utility model of regulation and characterized broadcasters as "'public trustees' who were 'privileged' to use a scarce public resource"—the public airwaves and the broadcast spectrum.[21] The emphasis was that licensed broadcasters had, in effect, "social responsibilities."[22] The overall goal was to ensure that "the interest, the convenience, and the necessity of the listening public," and not that of "the individual broadcaster or the advertiser," was "first and foremost."[23] We will return to these principles in the final part of the Essay but first need to briefly examine how they played out over time.

In the late 1970s and continuing in the 1980s, under Chairman Mark Fowler, the FCC began to revisit the traditional interpretation of the public interest with respect to the communications industry and to emphasize that regulation was only necessary "when the marketplace clearly fails to protect the public interest, but not when there is only a potential for failure."[24] At this time, the FCC set a higher threshold for regulation, reasoning that the increase in the number of broadcasting stations and other communications providers nullified the scarcity of the airwaves rationale for regulation. What the FCC saw instead was that particular stations were meeting the needs of particular segments of the public, and thus there was less need for one station to serve the interests of all listeners or viewers.[25] Additionally, the FCC believed that the public service role was part of broadcasters' culture and that the audience would demand that broadcasters serve the public,[26] which also lessened the need and rationale for government regulation. Democratic members of Congress, such as Edward Markey (D-MA) and John Dingell (D-MI), disagreed with the FCC's deregulatory moves, retaining the perspective that broadcasters were "licensees and trustees of the public airwaves" who should serve the public interest and that the market was not able to compel broadcasters to carry out these responsibilities.[27]

---

20. Erwin G. Krasnow & Jack N. Goodman, *The "Public Interest" Standard: The Search for the Holy Grail*, 50 FED. COMM. L.J. 605, 609 (1998) (quoting 67 CONG. REC. 5479 (1926) (statement of Rep. White)).

21. *Id.* at 610.

22. *Id.* at 626.

23. *Id.* at 611 (quoting FED. RADIO COMM'N, ANNUAL REPORT 166 (1928)).

24. *Id.* at 616.

25. *Id.* at 632.

26. *Id.*

27. Neal Devins, *Congress, the FCC, and the Search for the Public Trustee*, 56 L. & CONTEMP. PROBS. 145, 150 (1993) (citing *Straight Talk from Chairman Dingell*, BROADCASTING, Feb. 16, 1987, at 31).

Telecommunications also experienced a deregulatory wave in the 1980s. Nicholas Economides recounts that, historically, regulation, predominantly in the guise of anti-trust regulations, was seen as appropriate in the telecommunications sector for four reasons: the market could not bring about competitive outcomes; deviation from economic efficiency was socially desirable; social and private benefits were distinct; and there was a need to coordinate technical standards.[28] The 1934 Telecommunications Act laid the groundwork for federal regulation and established the FCC's jurisdiction over telecommunications as a common carrier service.[29] Until 1981, AT&T dominated all aspects of US telecommunications—local and long-distance lines and revenue, equipment (Western Electric), and research (Bell Labs)—and achieved near monopoly status.[30] Although the public interest objective was somewhat vague, regulators agreed that basic local phone service or "universal service" was desirable and even necessary from a public interest perspective.[31] By the 1970s, more than ninety percent of U.S. households had telephone service.[32] However, the Justice Department alleged that AT&T and the Bell system acted to limit competition through its monopoly on equipment, long-distance service, and local service and brought a major antitrust suit against AT&T in 1974, resulting in a settlement in 1984 in which AT&T retained the long-distance network and divested itself of seven regional telephone companies.[33] This settlement recognized that local telecommunications services had the characteristics of a natural monopoly while competition would likely flourish in long distance services.[34]

The story of telecommunications deregulation is fascinating but far too complex and intricate to convey in depth here. It is relevant to examine the trajectory of public interest concepts, however, so a brief overview is appropriate. The 1996 Telecommunications Act attempted to restructure the

28. Nicholas Economides, *Telecommunications Regulation: An Introduction*, *in* THE LIMITS OF MARKET ORGANIZATION 48, 50 (Richard R. Nelson ed., 2005).

29. Robinson, *supra* note 18, at 3, 18. The term "common carrier" has a long legal history dating back to Roman law and English common law with the intent of conveying that a service was open to the general public without discrimination. Title II of the Communications Act of 1934 regulated telecommunications services as common carriers. Eli Noam identified "the following factors are important in determining common carriage: [s]ervice is regular[;] [c]ustomers are not readily predictable and are changeable[;] [t]he carrier solicits business from the general public, for example by advertising[; and] law and regulations define the responsibilities of the parties." Eli M. Noam, *Beyond Liberalization II: The Impending Doom of Common Carriage*, 18 TELECOMM. POL'Y 435, 437–38 (1994).

30. Economides, *supra* note 28, at 55.

31. *Id.* at 51–52.

32. *Id.* at 54.

33. *Id.* at 54–55.

34. ROBERT W. CRANDALL, AFTER THE BREAKUP: U.S. TELECOMMUNICATIONS IN A MORE COMPETITIVE ERA 8–9 (1991).

U.S telecommunications sector and to "preserve and advance universal service,"[35] which included high quality service at low rates, access to advanced services in all states, rural access, and access to advanced services for schools, health care facilities, and libraries.[36] These goals continue to guide the expansion of broadband Internet services in the United States[37] and have recently led the FCC to reclassify internet service providers ("ISPs"), or providers of broadband Internet access service ("BIAS"), as telecommunications providers. Previously, ISPs were classified as "information services" under Title I of the 1996 Telecommunications Act,[38] but the FCC's 2015 Open Internet Order reclassified them as telecommunications providers, services, or "common carriers" under Title II of the Communications Act and Section 706 of the Telecommunications Act of 1996.[39] This reclassification broadens the FCC's authority to regulate certain aspects of the activities of ISPs in the tradition of a responsibility to operate in the "public interest."

III. THE LANDSCAPE OF THE TWENTY-FIRST CENTURY INTERNET

As the Internet began to evolve from a community of researchers to a global commercial network, the U.S. government made a conscious policy decision to step back and let it evolve without government regulation. In outlining the Clinton administration's position as reflected in the report of the National Information Infrastructure ("NII") Task Force, Vice President Gore provided five principles to guide policy:

- Encourage Private Investment
- Provide and Protect Competition
- Provide Open Access to the Network
- Take Action To Avoid Creating a Society of Information "Haves" and "Have Nots"
- Encourage Flexible and Responsive Governmental Action[40]

35. Economides, *supra* note 28, at 65 (quoting Telecommunications Act, 47 U.S.C. § 254(b) (2012)).

36. *Id.*

37. Priscilla M. Regan, *Oh What a Tangled Web: Implementation of Broadband Assistance Grants*, *in* GOVERNING UNDER STRESS: THE IMPLEMENTATION OF OBAMA'S ECONOMIC STIMULUS PROGRAM 85, 85 (Timothy J. Conlan et al. eds., 2017).

38. Verizon v. FCC, 740 F.3d 623, 650 (D.C. Cir. 2014).

39. *In re* Protecting and Promoting the Open Internet, 30 F.C.C. Rcd. 5601, 2015 WL 1120110 (2015); *see also Open Internet*, FED. COMM. COMM'N, https://www.fcc.gov/general/open-internet (last visited May 17, 2017) (providing background information and documents).

40. Al Gore, U.S. Vice President, Remarks Delivered at the Superhighway Summit (Jan. 11, 1994), https://clinton1.nara.gov/White_House/EOP/OVP/other/superhig.html; INFO. INFRASTRUCTURE TASK FORCE, NAT'L TELECOMM. & INFO. ADMIN., THE GLOBAL INFORMATION

Privacy was one of several topics discussed by the NII Task Force and, in April 1997, it released an options paper for public comment raising the question of how best to implement FIPs "that balance the needs of government, commerce, and individuals, keeping in mind both our interest in the free flow of information and in the protection of information privacy?"[41] The Task Force noted the possibility that "demand could foster a robust, competitive market for privacy protection. . . . [and] that privacy could emerge as a market commodity in the Information Age," but also discussed the ways in which the government could facilitate the development of a privacy market and enforce self-regulation, and the possibility of the creation of a federal privacy entity.[42] Based in part on the report of the Task Force, the Clinton Administration's *Framework for Global Electronic Commerce* concluded: "We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, *but if effective privacy protection cannot be provided in this way, we will reevaluate this policy*."[43]

Since these early discussions, the prevailing policy approach in the United States has been one of limited government regulation over both classic market conditions (entry, exit, price) and over privacy protections. But there is increasing recognition that competition on the Internet has actually concentrated power in the hands of a few key actors—particularly ISPs and what are referred to as "edge intermediaries," such as Facebook and Google. Likewise, there is increasing recognition that self-regulation has not effectively protected online privacy and that a privacy market has not evolved.[44] Instead, individuals' private information has been commodified and, through online advertising, provides the foundation for "free" websites. As Frank Pasquale similarly points out:

> It would be nice to believe that market forces are in fact promoting optimal levels of privacy. It would also be comforting

INFRASTRUCTURE: AGENDA FOR COOPERATION (1995), https://www.ntia.doc.gov/report/1995/global-information-infrastructure-agenda-cooperation.

41. INFO. POLICY COMM., NAT'L INFO. INFRASTRUCTURE TASK FORCE, OPTIONS FOR PROMOTING PRIVACY ON THE NATIONAL INFORMATION INFRASTRUCTURE (1997), https://aspe.hhs.gov/report/options-promoting-privacy-national-information-infrastructure.

42. *Id.*

43. THE WHITE HOUSE, A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE, https://clinton4.nara.gov/WH/New/Commerce/read.html (last visited May 17, 2017) (emphasis added).

44. *See, e.g.*, Peter Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (U.S. Dep't. of Commerce ed., 1997), https://www.ntia.doc.gov/report/1997/privacy-and-self-regulation-information-age; Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1061 (2009).

> if antitrust law indirectly promoted optimal privacy options by assuring a diverse range of firms that can compete to supply privacy at various levels (and in various forms). But this position is not remotely plausible.[45]

With respect to large Internet actors, particularly the ISPs but also Apple, Google, and Facebook, the key policy question is how best to characterize the roles they currently play. Are these companies, for example, establishing the infrastructure of modern communication? Are they providing essential services in conducting modern lives? Do they provide the foundations over which daily communications and transactions occur? These questions regarding the implications of the size and scale (global) of these companies, as well as the pivotal roles they play in modern life, have generated something of a rethinking of whether free market competition and a largely hands-off role by government regulators is still appropriate. If the answers to these questions are affirmative, then some form of government regulation acknowledging those roles can be justified.

Several privacy scholars have recently begun to engage in analysis of how these firms and their role in modern economic and social life should be defined; they more often than not conclude that the role of these firms is critical and not easily substituted by other companies or actors. Jeffrey Rosen, for example, points out that "social norms are not something that Facebook reflects. On the contrary, Google and Facebook have a crucial role in shaping those social norms."[46] Taking a somewhat different approach, Pasquale argues that these firms are:

> less services than they are *platforms* for finding services (and, occasionally, goods). Facebook, Google, and even Internet service providers ("ISPs") might be thought of less as sellers of particular end services than as advisors or gatekeepers, or connectors between users and what they want. In this intermediary role, Internet companies are far closer to health insurers or mortgage brokers than they are to sellers of products or services.[47]

Deborah Johnson and I similarly raised questions about the status of both Google and Facebook.[48] If Google is a search engine with a mission of

---

45. Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1010 (2013).

46. Jeffrey Rosen, *The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google*, 80 FORDHAM L. REV. 1525, 1535 (2012).

47. Pasquale, *supra* note 45, at 1015 (footnote omitted) (citing Ioannis Lianos & Evgenia Motchenkova, *Market Dominance and Search Quality in the Search Engine Market*, 9 J. COMPETITION L. & ECON. 419, 421 (2013)).

48. Priscilla M. Regan & Deborah G. Johnson, *Policy Options for Reconfiguring the Mirrors*, *in* TRANSPARENCY AND SURVEILLANCE AS SOCIOTECHNICAL ACCOUNTABILITY: A HOUSE OF MIRRORS 162, 184 (Deborah G. Johnson & Priscilla M. Regan eds., 2014).

delivering knowledge (along the lines of a twenty-first century library), then we might consider Google as something like a public utility or quasi-public trust. Moreover, it is important to acknowledge that, at the same time as delivering "free" knowledge to its users, Google is also delivering users as products to its paying customers: advertisers.[49] With respect to Facebook, we asked whether it is "the Ma Bell of the twenty-first century—and should it be regulated as such? . . . [H]as Facebook become public space, and should it be regulated in accordance with public trustee principles?"[50]

In testimony before the Senate Committee on Commerce, Science, and Transportation, Paul Ohm cited four justifications for requiring ISPs (BIAS providers) to provide a higher standard of protection for information privacy: the history of common carriers' responsibility "to respect the privacy of the information they carried"; the "relative lack of choice" consumers have; the "privileged place" ISPs have in the network (gatekeeper, bottleneck); and the sensitivity traditionally accorded information such as communications, reading habits, and location.[51] Ohm noted that other online entities demonstrate some of the same characteristics such as social networking sites that "carry exceptionally sensitive information and exhibit network effects and insufficient data portability that limit customer choice and exit."[52]

There is some interest on Capitol Hill, in the regulatory agencies, and in the states in revisiting how to classify these firms and what policy approach is warranted given their size and scale. Congressional committees held a number of hearings on a possible antitrust approach to Google in September 2012. In February 2012, thirty-six state attorneys general addressed the dominant position that Google has in both the search engine and email environments, and the lack of choice consumers actually have: "It rings hollow to call their ability to exit the Google products ecosystem a 'choice' in an Internet economy where the clear majority of all Internet users use—and frequently rely on—at least one Google product on a regular basis."[53]

49. *Id.* at 167.

50. *Id.* at 168–69.

51. *How Will the FCC's Proposed Privacy Regulations Affect Consumers and Competition? Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 114th Cong. 2–5 (2016) (written statement of Paul Ohm, Professor, Georgetown University Law Center and Faculty Director, Georgetown Center on Privacy and Technology), http://www.commerce.senate.gov/public/index.cfm/hearings?Id=1A0FC3ED-B203-4B2F-8892-DF01C1C7001E&Statement_id=720B518C-FB11-4448-9BD6-A072D37B398D.

52. *Id.* at 9.

53. Rebecca DiLeonardo, *State Attorneys General Concerned About Google Privacy Policy*, JURIST: PAPER CHASE (Feb. 23, 2012, 12:25 PM) (citing Press Release, Nat'l Ass'n Attys. Gen., Attorneys General Express Concerns Over Google's Privacy Policy (Feb. 22, 2012)), http://www.jurist.org/paperchase/2012/02/state-attorneys-general-concerned-about-google-privacy-policy.php.

Both the FTC and FCC have recently come close to imposing more regulations on these large actors as illustrated by the FTC's antitrust investigations of Google,[54] and the FCC's consideration of whether its net neutrality rules empowered it to impose requirements on Google, Facebook, and other Internet companies, as well as ISPs.[55] Although neither the FTC nor the FCC took action against these "edge players," it is likely that more such proposals will be made in the near future.

The question now is how best to provide for effective information privacy protection in this new landscape of the twenty-first century Internet. Traditional self-regulation with occasional prodding from government agencies, congressional committees, consumer and privacy groups, and state attorneys general has yielded not only a patchwork of laws and regulations, but also an inexplicable morass of confusion for the individual.[56]

IV. NEW CONCEPTS FOR INFORMATION PRIVACY PROTECTION—PUBLIC TRUSTEE

In this final Part of the Essay, I will argue that the public trustee regulatory regime, rather than the anti-trust regime or the environmental externality regulatory regime, will provide a more robust path to effective information privacy protection. Three arguments provide the rationale for this conclusion: First, the large online players are operating at the scope and scale where "public interest, convenience, and necessity" demand that they be more regulated. Second, a public trustee approach avoids the somewhat messy issues of proving "concentration" and anti-competitive behavior entailed in antitrust regulation. Third, the public trustee approach draws upon the link between privacy and trust that has emerged from public opinion surveys and the academic literature on privacy.

The first argument for a public trustee type of regulatory regime entails a realistic recognition, as noted above, of the size, scale, and influence of these so-called "edge players." Evidence for this comes in sheer numbers alone. Facebook reported in November 2016 that about 1.8 billion people

54. Miguel Helft, *Google Confirms F.T.C. Antitrust Inquiry*, N.Y. TIMES: BITS (June 24, 2011, 1:59 PM), https://bits.blogs.nytimes.com/2011/06/24/google-confirms-f-t-c-antitrust-inquiry/?_r=0.

55. Edward Wyatt, *F.C.C., in a Shift, Backs Fast Lanes for Web Traffic*, N.Y. TIMES (Apr. 23, 2014), https://www.nytimes.com/2014/04/24/technology/fcc-new-net-neutrality-rules.html?partner=socialflow&smid=tw-nytimesbusiness.

56. *See* Colin J. Bennet, Priscilla M. Regan & Robin M. Bayley, *If These Canadians Lived in the United States, How Would They Protect Their Privacy?*, FIRST MONDAY, no. 3, 2017, http://firstmonday.org/ojs/index.php/fm/article/view/6817.

around the world log on to Facebook every month.[57] According to a Pew survey, forty-four percent of adults in the United States report that they get their news from Facebook.[58] The implications of the role of platforms or edge providers have been most starkly apparent in the recent debates regarding the role that Facebook and Google played in spreading "fake news" during the 2016 election. News report after news report[59] criticized the influence these companies had and the fact that that influence was generated by algorithms that few understand and by a business model that would appear to enable, if not reward, fake news. Zeynep Tufekci pointed out in an op-ed in the *New York Times* that:

> Only Facebook has the data that can exactly reveal how fake news, hoaxes and misinformation spread, how much there is of it, who creates and who reads it, and how much influence it may have. Unfortunately, Facebook exercises complete control over access to this data by independent researchers. It's as if tobacco companies controlled access to all medical and hospital records.[60]

Similarly, Farhad Manjoo wrote: "It's time to start recognizing that social networks actually are becoming the world-shattering forces that their boosters long promised they would be—and to be unnerved, rather than exhilarated, by the huge social changes they could uncork."[61]

To this point, platforms have themselves assumed some responsibility for policing or controlling the content on their sites. In the mid-2000s, the deputy general counsel at Google had the authority and responsibility for determining, both for Google in the United States and Google in other countries, what content could be displayed and what could not.[62] This role,

57. *Facebook, Inc. (FB) Q3 2016 Earnings Call*, NASDAQ (Nov. 2, 2016, 5:00 PM), http://www.nasdaq.com/aspx/call-transcript.aspx?StoryId=4018524&Title=facebook-fb-q3-2016-results-earnings-call-transcript.

58. Jeffrey Gottfried & Elisa Shearer, *News Use Across Social Media Platforms 2016*, PEW RES. CTR. (May 26, 2016), http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/.

59. *See, e.g.*, Caitlin Dewey, *Facebook Fake-News Writer: 'I Think Donald Trump Is in the White House Because of Me'*, WASH. POST (Nov. 17, 2016), https://www.washingtonpost.com/news/the-intersect/wp/2016/11/17/facebook-fake-news-writer-i-think-donald-trump-is-in-the-white-house-because-of-me/?utm_term=.e4cfdda7ac74; Mike Isaac, *Facebook, in Cross Hairs After Election, Is Said to Question Its Influence*, N.Y. TIMES (Nov. 12, 2016), https://www.nytimes.com/2016/11/14/technology/facebook-is-said-to-question-its-influence-in-election.html; Nick Wingfield et al., *Google and Facebook Take Aim at Fake News Sites*, N.Y. TIMES (Nov. 14, 2016), https://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html?_r=0.

60. Zeynep Tufekci, Opinion, *Mark Zuckerberg Is in Denial*, N.Y. TIMES (Nov. 15, 2016), https://www.nytimes.com/2016/11/15/opinion/mark-zuckerberg-is-in-denial.html.

61. Farhad Manjoo, *Social Media's Globe-Shaking Power*, N.Y. TIMES (Nov. 16, 2016), https://www.nytimes.com/2016/11/17/technology/social-medias-globe-shaking-power.html.

62. Rosen, *supra* note 46, at 1536.

referred to as the "Decider," placed enormous decisionmaking power over what people around the world would see and not see, and control over when and how people could speak or when they would be censored. Although this power was generally used rather wisely at the time, as Jeffrey Rosen argues: "You might be uncomfortable with the idea of allowing a single woman, a Decider, to make these incredibly contextual and difficult free speech decisions for the globe, but the truth is that this Decider model, as inadequate as it may be, may be better than the alternatives."[63] From a policy options perspective, the alternatives have not been fully explored yet, for a number of reasons, the time for exploring options seems to be now.

Both privacy protections and content regulation are central to the principles of "social responsibility" that underlined the original rationale for public trustee regulation. The evidence seems to demonstrate that self-regulation and a system of privacy notices does not effectively protect information privacy. The evidence also seems to show that self-regulation or no regulation is not effective to ensure content that does not undermine the integrity of something as fundamental to the democratic process as a presidential election. Thus, some regulation to ensure that companies serve the "public interest, convenience and necessity" seems justified.

A second argument for a public trustee type of regulatory regime is that it avoids the often-messy arguments entailed in antitrust regulation. Such arguments often get entangled in lengthy court cases and settlements, rely on detailed and unfathomable financial analyses, and are opaque for the American public. Beginning in 2010, both the FTC and the European Union ("EU") engaged in a number of antitrust investigations, including whether Google was acting in an anticompetitive manner and prioritizing search results towards Google-owned companies. Given the difficulties of finding clear and convincing evidence of discriminatory behavior and practices towards competitors, and the difficulties of predicting the dynamics of the innovative information marketplace, antitrust allegations are fraught with challenges.[64]

Such challenges played out in the FTC investigation of Google which, after three years of gathering evidence, holding hearings, and analyzing the complex record, resulted in some minor concessions on Google's part but no formal charges. By 2016, the European Commission had pursued five different antitrust investigations into Google, three of which resulted in formal charges. All indications are that the EU will not back off its inquiries and that countries such as France, where there is litigation over the "right to

63. *Id.*

64. Geoffrey A. Manne & Joshua D. Wright, *Google and the Limits of Antitrust: The Case Against the Case Against Google*, 34 HARV. J.L. & PUB. POL'Y 171, 209, 184 (2011).

be forgotten," and Italy will continue to scrutinize Google's activities.[65] In mid-2016, the FTC appeared to be considering reopening its investigation as a result of criticisms that Google is not a neutral gateway to information on the Internet. At an April 2015 congressional hearing, Senator Richard Blumenthal (D-Conn.) spoke as follows to the possibility of renewed FTC investigations: "While the company is a great American success story, their position in the marketplace has led to legitimate questions about whether they have used their market power to disadvantage competitors unfairly and ultimately limit consumer choice."[66]

Given the enormous time investment and significant financial and personnel costs that antitrust investigations entail for both government regulators and companies such as Google and Facebook, it may be to the advantage of both to pursue a less adversarial path to resolving these questions. In this sense, both regulators and companies may prefer to consider whether a public trustee style regime provides advantages. The FCC's recent actions with regard to privacy requirements for ISPs based on the sensitivity of the information—as well as requirements for transparency, data security, and data breach notifications—may provide a trial assessment to see whether an alternative such as this would be more advantageous than the antitrust route.[67] Both Google and Facebook successfully resisted being included in the FCC's privacy actions, but depending on how the FCC regulations play out, it is possible that a change on the companies' part and/or on the part of consumer and privacy advocates may result in inclusion of such edge players.

A third argument for the public trustee approach is that it acknowledges the importance of the fundamental connection between privacy and trust that has been demonstrated to be necessary in the information economy and Internet landscape more generally. Neil Richards and Woodrow Hartzog make an interesting argument, consistent with my proposal here, to refocus privacy from a protection against bad things to an enabler of trust relationships, which would benefit both data subjects and data holder.[68] They apply the principle of "fiduciary duties" in much the way that I am thinking

65. Natalia Drozdiak & Sam Schechner, *EU Files Additional Formal Charges Against Google*, WALL ST. J., http://www.wsj.com/articles/google-set-to-face-more-eu-antitrust-charges-1468479516 (last updated July 14, 2016).

66. Nancy Scola, *Sources: Feds Taking Second Look at Google Search*, POLITICO (May 11, 2016, 2:38 PM), http://www.politico.com/story/2016/05/federal-trade-commission-google-search-questions-223078.

67. Press Release, Fed. Commc'ns Comm'n, FCC Adopts Broadband Privacy Rules to Give Broadband Consumers Increased Choice, Transparency and Security for Their Personal Data (Oct. 27, 2016), https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules.

68. Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016).

of public trustee in that they would similarly move privacy principles "from procedural means of compliance for data extraction towards substantive principles to build trusted, sustainable information relationships."[69] As they convincingly point out:

> Rather than encouraging trust, modern American privacy law encourages companies to profit in short-sighted ways by extracting as much value as possible from personal data in the short term. As long as companies don't cause a narrow set of legally recognized, largely financial harms, they are essentially free to set up the terms of information relationships any way they wish.[70]

Public opinion surveys from the 1980s onwards reveal that the public does not trust organizations "to collect and use information about people like you in a responsible way," with the lowest levels of trust in sectors that Americans associate with data collection and monitoring.[71] Such trust is not only important to individuals who are data subjects but also to the organizations collecting this information and is critical to both overall trust in government and trust in the digital economy. As Hirsch points out:

> Overall user trust in the digital economy is not only a vital resource; it is also an open-access, partially rivalrous one. No one can fence it off. Particular companies may enhance, or deplete, overall user trust in society. . . . But, in the absence of laws or other forms of social control, [particular companies] cannot prevent others from dipping into the well of overall user trust, or from diminishing it through abusive behaviors.[72]

The asymmetries in the data subject-data holder dynamic and the essential role that trust plays in this relationship have long been recognized, have gotten worse over time, and need to be readdressed. In analyses of a number of complex systems designed for purposes of surveillance or transparency, we found, "trust relationships are often ill defined or incompletely understood and trust is often compromised . . . . The individual becomes caught in a web of cascading mirrors, sending her into relationships

69. *Id.* at 431–32.

70. *Id.* at 434.

71. REGAN, *supra* note 6, at 65. Such questions were asked in a series of Louis Harris and Associates and Alan F. Westin opinion polls in the 1980s–1990s and more recently in a series of Pew Research opinion polls. *See, e.g.*, *id.* at 50–60 (discussing surveys); MARY MADDEN & LEE RAINIE, PEW RES. CTR., AMERICANS' ATTITUDES ABOUT PRIVACY, SECURITY AND SURVEILLANCE (2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/; Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW RES. CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

72. Hirsch, *supra* note 7, at 84.

over which she has no control, no expectations, and no basis of trust."[73] With an emphasis on data holders as public trustee, a concern with identifying and justifying "privacy harms" would not be part of policy discussions, as also pointed out by Richards and Hartzog.[74] Rather than focusing on the negative effects of information collection and use, policy discussions would shift attention to determining what kinds of information practices serve a public interest in an information economy.

Finally, I will consider some of the implications of an information privacy regulatory regime based on public trustee principles of "public interest, convenience and necessity." As noted above, the current privacy protection regime based on the FIPs and self-regulation overburdens the individual with tasks that are unrealistic, resulting in a system that is ineffective, causes cynicism and frustration among individuals, requires episodic prodding by federal regulators with inadequate power, and oftentimes leaves companies in a defensive and uncertain position. Under such circumstances, no one wins—not the individual, not the government, and not the companies. At the same time, further analysis of the personal information environment leads many to conclude that information privacy actually has many of the characteristics of a public good, which provides a rationale for rethinking a public trustee approach for protecting information privacy. So how might this play out?

First, it is important to recognize that, to some extent, such a shift actually entails something of a rethinking of Internet governance more generally. The development of the Internet has been something of a work in progress—without top-down planning and largely dependent on cooperative arrangements among self-identified affected private and public parties. The principles and regulations guiding this organic development have largely emerged through the process of development—first, by primarily addressing administrative (such as, system of domain names) and technical (such as, interoperability) concerns. More social principles were regarded as unwise and irrelevant, as perhaps best articulated in John Perry Barlow's *A Declaration of the Independence of Cyberspace*, which says to the governments of the world:

> We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all

73. Priscilla M. Regan, *Trust in a House of Mirrors?*, *in* TRANSPARENCY AND SURVEILLANCE AS SOCIOTECHNICAL ACCOUNTABILITY: A HOUSE OF MIRRORS 146, 159 (Deborah G. Johnson & Priscilla M. Regan eds., 2014). The systems examined include: Campaign Finance Disclosure, Secure Flight, American Red Cross, Google and Facebook. *Id.*

74. Richards & Hartzog, *supra* note 68, at 459.

> our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.[75]

The reality that evolved over the twenty years since this was written is quite different than what the pioneers of Cyberspace envisioned. Rather than a parallel universe for virtual communities providing more freedom and creativity than the physical world, Cyberspace has developed as an adjunct of the physical world dominated and organized by the same large organizations that exist in that world.

Second, perhaps more appropriately termed "hopefully," the process of formulating information privacy policies—as well as those for free content regulation and law enforcement or intelligence access—would be less adversarial under a public trustee regime. Rather than long drawn out lawsuits with zero-sum stakes, a focus on the social responsibility of large Internet players might redirect attention from particular, competing stakeholder interests to the broader common or shared interests of all parties. To a certain extent, the development and roles of privacy officers[76] in private and public organizations illustrate the type of dynamic that might emerge under a public trustee regime—but with their role elevated and substantiated by government sanctions and oversight in a more cooperative corporatist process than either self-regulation or government regulation entail. How this might develop will require more research and analysis, but seems to be a path worth pursuing.

75. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence.

76. KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE (2015).