A DESIGN FOR PUBLIC TRUSTEE AND PRIVACY PROTECTION REGULATION[1]

*Priscilla M. Regan**
George Mason University

I. INTRODUCTION

Privacy scholars have long recognized and documented the shortcomings of the fair information practice principles (herein "FIPPs") of "notice, choice and consent" approach to protect information privacy. These shortcomings are even more pronounced in today's political and social world for three reasons. First, big data and its concomitant algorithmic power have radically changed the nature and effects of personal information processing, challenging FIPPs style regulation in fundamental ways. Second, the broad recognition of the social importance of privacy, especially its importance to

* Priscilla M. Regan is a Professor in the Schar School of Policy and Government at George Mason University. Prior to that, she was a Senior Analyst at the Congressional Office of Technology Assessment. [1] Earlier drafts of this paper were presented at the Amsterdam Privacy Conference in October 2018 and the Privacy Law Scholars Conference in May 2019. The author would like to acknowledge the helpful comments received at these conferences from Lisa Austin, Jacquelyn Burkell, Julie Cohen, Bob Gellman, Woody Hartzog, Sarah Igo, Cameron Kerry, Siona Listokin-Smith, Mary Madden, Bill McGeveran, Deirdre Mulligan, Kobbi Nissim, Jim Rule and Valerie Steeves. The author also appreciates the research assistance of Caroline Ball, an MPA student at George Mason University.

democracy, undercuts the rationale for an individual rights approach and renders FIPPs even more problematic. Third, the emergence of large internet platforms controlling how individuals experience social, political, and economic life has rendered a FIPPs approach to protecting privacy obsolete and ineffective. Several scholars have examined the rationale for and potential effectiveness of policy alternatives to FIPPs, including alternatives such as an anti-trust approach or regulation modeled on environmental regulation. In a 2017 essay in the *Maryland Law Review*, I provided a preliminary investigation of whether and how the public trustee concept might be applied to information privacy policy. In that piece, as here, I was using the term "public trustee"[2] in its broadest sense to represent a position of trust with a legal obligation to use its powers solely for the benefit of the public—in this case, that personal data would be used in a fair and responsible manner. My thinking paralleled that of others arguing that an individual rights approach to privacy protection was ineffective and that instead, obligations should be placed on those organizations collecting and using data. Neil Richards and Woody Hartzog emphasized the importance of "trust,"[3] while Jack Balkin and Lindsey Barrett spoke of "information fiduciaries."[4] At the same time that scholars and policymakers are exploring policy alternatives to FIPPs, larger issues regarding the power of major internet actors (ISPs and platforms/edge players) and their lack of accountability to the public have surfaced. Most recently, this has arisen in the context of "fake news," the explosion of biased and inaccurate information on the internet and its effect on public discourse and democratic participation, as well as the implications of reversing net neutrality regulations.

This tide of current events has brought attention to the fact that the fundamental policy problem regarding today's major internet actors is "private power and American democracy."[5] During the transition from a largely agricultural based economy to an industrial based economy, a number of regulatory regimes, rationales and institutions (e.g., anti-trust, public utilities, common carriers, consumer protection) were developed to control the negative effects of the private power exercised by major

---

[2] *See generally* Priscilla M. Regan, *Reviving the Public Trustee Concept and Applying it to Information Privacy Policy*, 76 MARYLAND L. REV. 1025 (2017).

[3] *See generally* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L REV. 431–472 (2016); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L. J. 1180 (2017).

[4] *See generally* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1185 (2016); Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE L. REV. 1057 (2019).

[5] GRANT MCCONNELL, PRIVATE POWER AND AMERICAN DEMOCRACY, New York: Knopf (1966).

economic actors of that time (e.g., railroads, communication companies). To a large extent, and not surprisingly, current discussions about possible policy solutions to the problems posed by new actors wielding private power in democratic systems have tended to use the frameworks and ideas of earlier policy eras. But, as has also been recognized in policy discussions regarding information privacy and organizational interests, pouring new wine into old bottles is not always effective.[6] The limitations of the regulatory regimes of the industrial age to that of the information age are increasingly recognized and a range of scholars are exploring alternative regulatory schemes.[7]

At this time, there are three primary arguments being offered in current policy discussions regarding the rationales to curb the private power wielded over internet-based activities: (1) the real or potential anti-competitive behavior of key internet gatekeepers; (2) the commodification of personal information and ubiquity of privacy intrusions; and (3) the explosion of fake news or inaccurate and biased information particularly on social media sites. The debate on the first is focused on the policy solution of net neutrality. The debate on the second in the U.S. has focused on rethinking a sectoral FIPPs approach as well as a self-regulatory approach. Last, the debate on the third raises questions of censorship and First Amendment conflicts.

In this paper, I focus on the synergy that exists among the three rationales being offered for regulating internet-based actors and on the underlying problem of private power on the internet, a power that is fueled by personal information. I argue that if policymakers resolve the information privacy question effectively, that will, at a minimum, mitigate the problems of fake news and misinformation, which is highly dependent upon easy access to information about individuals' consumer practices, activities, interests, philosophical leanings/orientations, etc., so that messages can be targeted to particular subgroups in the population. If access to such data is removed, it becomes far more difficult to target messages. At the same time if policymakers resolve the information privacy question, that will also reduce the control and discretion that major internet actors gain from the personal information they have access to and will decrease one element of their competitive advantage. Given that leverage, it seems that establishing

---

[6] Horace E. Anderson, Jr., *The Privacy Gambit: Toward A Game Theoretic Approach to International Data Protection*, 9 VAND. J. OF ENT. & TECH. L. 1, 11 (2006).

[7] *See, e.g.*, Julie E. Cohen, *The Regulatory State in the Information Age*, 17 THEORETICAL INQUIRIES IN L. 369 (2016); Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133 (2017); Orly Lobel, *Law of the Platform*, 101 MINN L. REV. 87 (2016); Hal J. Singer, *Paid Prioritization and Zero Rating: Why Antitrust Cannot Reach the Part of Net Neutrality Everyone is Concerned About*, THE ANTITRUST SOURCE, Aug. 2017, 1; Frank Pasquale, *Tech Platforms and the Knowledge Problem*, 2 AM. AFF. 3-16 (2018); K. Sabeel Rahman, *Regulating Informational Infrastructure: Internet Platforms as the New Public Utilities*, 2 GEO. L. TECH. REV. 234 (2018).

an effective scheme to protect information privacy should be a priority.

Further, this paper expands upon my earlier analysis of the applicability of a public trustee scheme or regulation and explores how a public trustee based regulatory regime might be designed in an era of big data and how it might be presented to gain political support. The paper first briefly examines the three reasons that the FIPPs approach is no longer applicable or effective in today's personal information environment. Second, the paper reviews the current debate about regulating private power on the internet. Third, it provides an explanation for why resolving privacy issues will also reduce fake news and misinformation problems without censorship of information and may also mitigate some of the issues associated with anti-competitive behavior. Finally, this paper explores how and why a public trustee based regulatory regime is relevant in this area of controlling private power in a democracy and proposes institutional design features for an agency based on public trustee principles that might reduce the possibility for industry capture and over-politicization.

II. INADEQUACY OF FIPPS APPROACH

The traditional FIPPs approach to protecting privacy, similarly, enshrined in information privacy policies in virtually all countries with such policies—albeit with different schemes for enforcement—is primarily aimed at providing individuals with the means to protect their own privacy. For many years, scholars, privacy advocates, and policymakers have questioned the effectiveness of this approach, especially when enforcement relies on individual initiative and is not supplemented with agency action.[8] Survey research and precepts of behavioral economics support the finding that people do not read privacy notices informing individuals of organizational information practices.[9] The problems and shortcomings of the FIPPs approach have been well documented, but recently are receiving renewed, and more serious, attention for three reasons.

First, big data and algorithmic power have changed the nature and effects of personal information processing in ways that fundamentally

[8] *See generally* PRISCILA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (UNC Press, 1995); 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, 816–17 (2000); Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880–81 (2013); Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1038 (1999).

[9] *See generally* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 543 (2008); Alessandro Acquisti, *The Economics and Behavioral Economics of Privacy*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 76 (Julia Lane et al. eds., 2014).

challenge FIPPs-style regulation. The advent of big data and use of algorithms coupled with machine learning have generated scores of social science and law review articles pointing out the various effects of these developments on information privacy generally, and on existing regulations protecting privacy.[10] The techniques associated with big data enable new tools for generating data, designing data sets, culling the data for patterns and trends, and identifying either individual or group prototypes of behavior. Not only does big data entail collection and analysis of more and more refined data without individual knowledge, but big data also expands the power to influence, and restricts and predicts individuals' actions and the opportunities presented to an individual.[11] Privacy problems include controlling the collection and use of information about oneself, autonomy over decision-making, anonymity, choice in group associations, and discrimination or bias in decisions—raising not only classic FIPPs values of consent, choice, and transparency, but equally importantly related values of due process, equal protection, data security, and accountability.

Second, the broad recognition of the social importance of privacy, especially its importance to democracy, renders the FIPPs approach even more problematic. Since the mid-1990s, scholars across a number of disciplines have drawn attention to the reality that privacy is not just important to individuals but also critically important to society as a whole.[12] Recent developments over the last several years have underscored privacy's importance as a public value and its critical importance to democratic

---

[10] *See generally* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 153 (Houghton Mifflin Harcourt, 2013); JULIA LANE, VICTORIA STODDEN, STEFAN BENDER, & HELEN NISSENBAUM, PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT, xi (Cambridge U. Press, 2014); JULIA LANE, VICTORIA STODDEN, STEFAN BENDER, & HELEN NISSENBAUM, PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT, xi (Cambridge U. Press, 2014); Paul Ohm, *The Underwhelming Benefits of Big Data*, 161 U. PA. L. REV. 339, 339–340 (2013); Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 STAN. L. REV. 25, 25 (2013); Priscilla M. Regan, *Big Data and Privacy*, *in* ANALYTICS, POLICY AND GOVERNANCE 204 (Jennifer Bachner, Benjamin Ginsberg, & Kathryn Wagner Hill eds., 2017); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671, 671–72 (2016); Lisa M. Austin, *Towards a Public Law of Privacy: Meeting the Big Data Challenge*, 71 SUP. CT. L. REV. 540, 543 (2015).

[11] Ian Kerr & Jessica Earle, *Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy*, 66 STAN. L. REV. ONLINE 65, 66 (2013).

[12] *See generally* REGAN, *supra* note 8, at xiv; BEATE RÖSSLER, THE VALUE OF PRIVACY 1 (R.D.V. Glasgow trans., 2005); Valerie Steeves, *Reclaiming the Social Value of Privacy*, *in* LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY, AND IDENTITY IN A NETWORKED SOCIETY 191–208 (Kerr et al. eds., 2009); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY, ix (Harvard Univ. Press, 2008); JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 1 (Yale Univ. Press, 2012); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 3 (Stanford Univ. Press, 2010).

participation. Across the globe, more sophisticated collection and analysis of personal information by candidates, political parties, and interest groups have fostered polarization and partisanship.[13] Segmentation and the targeting of political messages to selected subgroups of the population undermine traditional notions of "the public" or a "body politic" which are fundamental to democratic citizenship. If information privacy is important to maintaining the integrity of the public in a democratic system of government, then a policy approach based on individual choice and consent is not an appropriate policy remedy.

Third, the emergence of large internet platforms controlling how individuals experience social, political, and economic life has rendered a FIPPs approach to protecting privacy obsolete and ineffective. There is growing recognition that the complex socio-technical systems on which much of modern life is organized are now exhibiting attributes of public infrastructures.[14] Alice Marwick and Danah Boyd see these technological shifts in the information and cultural landscapes creating "networked publics"[15] and necessitating a conceptualization of privacy that moves beyond an individualistic approach. Facebook, Google, and Amazon are the primary examples of the importance of socio-technical systems whose complex architectures and business models, scale and reach of their operations, and the huge number of people worldwide who use these systems underscore their infrastructural characteristics. Under these circumstances, privacy has to be established as a component of the network or infrastructure, including the various databases and interconnections that compose the network, and privacy is shared collectively by those in the network.[16]

III. ARGUMENTS FOR REGULATING PRIVATE POWER ON THE INTERNET

There are three primary arguments being offered today to curb the private power wielded over internet-based activities. These arguments are to some extent occurring on parallel tracks as they represent different, but arguably intersecting, concerns about aspects of the power of internet actors

---

[13] Colin J. Bennett, *Voter databases, Micro-targeting, and Data Protection Law: Can Political Parties Campaign in Europe as they do in North America*, 6 INT'L DATA PRIV. L. 261 (2016); Ira S. Rubinstein, *Voter privacy in the Age of Big Data*, 2014 WIS. L. REV. 861 (2014); Jacquelyn Burkell & Priscilla M. Regan, *Voting Public: Leveraging Personal Information to Construct Voter Preference*, *in* BIG DATA, POLITICAL CAMPAIGNING AND THE LAW (Normann Witzleb, et. Al ed., Routledge 2020) (2020).

[14] DEBORAH G. JOHNSON & PRISCILLA M. REGAN, TRANSPARENCY AND SURVEILLANCE AS SOCIOTECHNICAL ACCOUNTABILITY: A HOUSE OF MIRRORS (New York: Routledge, 2014).

[15] Alice E. Marwick & Danah Boyd, *Networked Privacy: How Teenagers Negotiate Context in Social Media*, 16 NEW MEDIA AND 1051, 1052 (2015).

[16] REGAN, *supra* note 8, at 243; Priscilla M. Regan, *Privacy and the Common Good: Revisited*, SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES (Beate Roessler & Dorota Mokrosinska eds., 2015).

and activities. The argument offered in this paper is that if policy effectively addresses the second concern, privacy intrusions, it will also address to some extent the first, anti-competitive behavior, and third, misinformation or "fake news," concerns. Imagine a Venn diagram of these three policy arguments or arenas. Data about individuals is the intersection in the middle of the diagram.

The first concern involves the real or potential anti-competitive behavior of key internet gatekeepers, especially internet service providers (herein "ISPs"), but also what are sometimes referred to as edge players/ platforms, including Google, Facebook, and Amazon. These two sets of actors are currently regulated by different agencies: the Federal Communications Commission (FCC) has jurisdiction over ISPs, but not over platforms, and the Federal Trade Commission (FTC) has jurisdiction over "unfair and deceptive trade practices" of platforms, but not ISPs.[17] Much of the debate about anti-competitive behavior has focused on the policy solution of "net neutrality"—the idea that providers of internet content should not be discriminated against in their ability to provide offerings to consumers and that users should have equal access to see any legal content they choose.[18] Evidence of horizontal and vertical consolidation of large online platforms and consolidation of ISPs has generated concern about possible blocking or discriminating amongst customers. For example, among ISPs, Time Warner Cable merged with Charter Communications in 2015, AT&T merged with Direct TV in 2015 and Time Warner in 2018, and Verizon merged with XO Communications in 2017. Among internet platforms, Google has acquired YouTube, Doubleclick, ITA, Waxe, and AdMob, while Facebook has acquired Instagram and WhatsApp, among others, and Amazon has acquired Whole Foods and Zappos. Net neutrality principles require ISPs to charge all content providers similarly and not to privilege large providers and customers to the detriment of smaller providers. In the U.S., debate over net neutrality has been contentious and partisan. In 2005, the FCC adopted a form of net neutrality or non-discrimination guidelines; from 2006 to 2009, Congress unsuccessfully considered a number of net neutrality rules; and in 2010, a Circuit Court ruled that the FCC did not have the authority to regulate ISPs.[19] In 2015, the FCC approved net neutrality rules, which were upheld by the U.S. Court of Appeals for the D.C. Circuit as within the FCC's jurisdiction, but then

[17] Jeffrey A. Eisenach and Ilene Knable Gotts, *Looking Ahead: The FTC's Role in Information Technology Markets*, 83 GEO WASH L. REV. (2015) 1876–1901.

[18] Jan Kramer, Lukas Wiewiorra, and Christoff Weinhardt, *Net Neutrality: A Progress Report*, 37 TELECOMM. POL'Y REV. (2013): 794–813.

[19] Jeffrey A. Hart, *The Net Neutrality Debate in the United States*, 8 J. OF INFO. TECH. & POL. 418–443 (2015).

repealed by the FCC in December 2017. On April 10, 2019, the House on a party-line vote reinstated net neutrality rules, which are unlikely to be passed by the Senate. California passed a net neutrality law in October 2018, which was challenged by the U.S. Department of Justice.

The second concern addresses the commodification of personal information and ubiquity of privacy intrusions. As discussed above, the policy solution of FIPPs is increasingly questioned and new approaches are being proposed. For example, in May of 2018, the European Union instituted a more active regulatory stance in the General Data Protection Regulation (herein "GDPR") which, among other things, requires all companies processing the personal data of data subjects residing in the Union, regardless of the company's location to: request consent in an intelligible and easily accessible form, with the purpose for data processing duly noted; provide notifications of data breaches without undue delay; supply a free electronic copy of all personal data held by the controller; and entitle the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.[20] Additionally, Article 22 of the GDPR prohibits the use of automated/algorithmic decision-making that produces "legally significant" or "similar effects," unless a human is involved in the process.[21] The institution of the GDPR, combined with continuing reports of large-scale data breaches, increased attention to potential discriminatory effects of algorithms, and the introduction of new products that are reliant upon the use of personal information, have generated renewed policy discussions in the U.S. as well. In 2018, California passed the California Consumer Privacy Act (herein "CCPA") (effective January 2020) that mirrors many of the requirements of the GDPR and adopts a more regulatory approach than traditional FIPPSs.[22] A number of congressional committees have held hearings, and several bills were introduced in 2018-2019, but all have stalled in committee.[23]

The third concern involves the explosion of inaccurate or biased information particularly on social media and blog sites and its influence in shaping the democratic process, not just in one country, but globally, through

[20] General Data Protection Directive, *Intersoft Consulting*, https://gdpr-info.eu/. (last visited 2020).

[21] *Id.*

[22] For discussion of the differences between the GDPR and CCPA, *see* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, GEO. L. FACULTY PUBLICATIONS AND OTHER WORKS 2190 (2019).

[23] *See, e.g.*, Senator Wyden's Consumer Data Protection Act; Senator Schatz's Data Care Act; Senator Rubio's American Data Dissemination Act; Senators Markey and Blumenthal's CONSENT Act; and Senator Klobuchar's Social Media and Privacy Protection and Consumer Rights Act. *See* Chander, *supra* note 22, at pp. 34–35 for a more complete list.

the messages that are circulated to subsets of the population who are most likely to be interested in or influenced by those particular messages. Concern about this issue intensified following the 2016 election in the U.S. as well as European elections and the rise of more radical right thinking around the world. These discussions have focused on the knotty and unpopular question of censoring information—a policy that in the U.S. is abhorrent under the First Amendment but is equally concerning in European countries. One critical issue, if any form of censorship is entertained, is who should be the appropriate party to make decisions about taking down internet content—the government, the company, or an objective third party?

The key policy question seems to be not whether the powerful players on the internet *should* be regulated, but instead *how best* to regulate them. This sentiment was expressed by Facebook's Mark Zuckerberg in answering a question posed by Senator Graham before the Senate Judiciary and Senate Commerce, Science, and Transportation committees when Zuckerberg replied "I think the real question, as the internet becomes more important in people's lives is what's the right regulation?"[24] Part of the difficulty in answering this question has focused on determining what kind of entity these major internet players are—are they media companies, technology companies, financial companies, publishing companies or some new hybrid? How this question is answered will determine whether major internet players are bound by the rules and oversight of the FTC, FCC, the Federal Elections Commission (FEC), or some other regulatory agency. Or perhaps a new entity designed to address the specific complications of their business models and activities is necessary altogether. The next section presents the argument that if policymakers focus holistically on the problem of internet privacy and on the development of effective policy solutions for this problem, these solutions will also serve to minimize and curtail the problems of misinformation and "fake news" on the internet and will at least mitigate some of the issues associated with anti-competitive behavior by large internet actors.

IV. THE CENTRAL ROLE OF PROTECTING INFORMATION PRIVACY

It is widely recognized that the business models of large internet companies rely upon the collection, use, and analysis of personal information. In exchange for "free" services—such as search engines, email, social networking connections, and navigation systems—individuals provide their personal information as they begin a relationship with the service and subsequently reveal their activities to the companies as they use

[24] Aja Romano, *Don't Ask Whether Facebook Can Be Regulated. Ask Which Facebook to Regulate*, VOX (2018), https://www.vox.com/technology/2018/4/12/17224096/regulating-facebook-problems.

that service. The data that companies acquire from their users enables them to refine the services they offer and to offer new or related services. Information about one person is also analyzed against the information of others who are similarly situated or whose activities or characteristics interact with that person. This enables internet companies to expand their insights into someone's preferences or needs by virtue of information about others whom the person associates with or resembles in some way and thus to make more and/or more refined offerings to the person.

The commodification of personal information and the information asymmetries of the personal information market that currently exists between individuals and internet companies are profound and obviate any ability for individuals to effectively exercise control over the use of their information. The economics or market context in which personal privacy is seemingly negotiated inevitably draws attention to a number of what might be termed "market failures" including: asymmetries in knowledge about how personal information flows, lack of transparency regarding data exchanges, and lack of knowledge about the short-term and long-term implications and costs to the individual.[25] In the era of "big data" and social networking sites, the personal information market is further complicated from a privacy protection perspective because the actions of other individuals, with whom one may or may not be associated, renders it impossible for individuals to procure reliable and complete information on the implications of revealing their information or engaging with a service that collects their information. On a number of online platforms, in particular social networking sites, one's own information privacy is dependent upon one's friends, friends of friends, professional colleagues, fellow members of political and interest groups, those who may have access to one's information and, perhaps more critically, those whose actions may affect the privacy of others in that group.[26] Moreover, these online platforms disclose information about your

[25] Joshua A. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385 (2015), https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1014&context=dlj_online; A. Michael. Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, U. ILL L. REV. 1713 (2015); 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 67–93 (2016); Priscilla M. Regan, *Response to Privacy as a Public Good*, 65 DUKE L.J. 51–65 (2016).

[26] Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 ISJLP 425 (2011); Solon Barocas & Helen Nissenbaum, *Big Data's End Run Around Anonymity and Consent*, *in* Julia Lane et. al., *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, CAMBRIDGE UNI. PRESS (2014); Paul Ohm, *Changing the Rules: General Principles for Data Use and Analysis*, in Julia Lane et. al., *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, CAMBRIDGE UNI. PRESS (2014); Regan, *supra* note 25.

activities within what they define as your social circle—based on algorithmic analyses and inferences about your preferences, social and political leanings, activities, use of time, etc. Examples here abound. Eventbrite, Evite, and other online invitation sites ask whether you want to see who else you know is coming or simply inform you who is coming—sharing with you information that these individuals likely did not know would be shared, as well as providing incentives for you to attend depending on who else was attending. Likewise, Instagram suggests people who you should follow—not at the initiative or desire of the person but based on Instagram's analysis of who you follow and who they are following.

Not only is personal information commodified, it is then analyzed by machine-based learning systems developed by data scientists to reveal even more information. Use of this data and algorithmic tools for culling the data are not restricted to nudging you within your social circle but, as was starkly revealed with respect to Facebook's activities in the 2016 American election, have also reached into areas fundamental to democracy.[27] These activities involve sophisticated targeted messaging along the lines of behavioral advertising commonly practiced in the commercial sector,[28] which companies argue are protected by the First Amendment.[29] As the discussion of policy problems posed by targeted messaging of biased or false information to sway voters' political views and votes ensues, the policy solution receiving the most attention focuses on some form of censorship or control over the content of messages. This has engendered further disagreement about what type of entity would be most appropriate to exert such control: the companies themselves, e.g., Facebook; a government body; or some independent third party. Not surprisingly, political views also color the debate and mask the pivotal role that personal information collection and use plays in causing both fake news/misinformation and the power wielded by major internet platforms.

The collection and use of data about individuals also play a pivotal role in the competitive advantage of ISPs and large internet platforms. Although ISPs appear not to have taken direct advantage of such information, the potential for it to engage in offering auxiliary services to individual customers or packaging such customers for online service providers does exist. Large internet platforms, however, do clearly take advantage of what they know about their customers in shaping the users' experience. Such

---

[27] *See* articles in Special Issue: Bennett, C. J. & Lyon, D. (2019). Data-driven elections: implications and challenges for democratic societies. *Internet Policy Review*, 8(4). DOI: 10.14763/2019.4.1433

[28] Burkell & Regan, *supra* note 13; Jacquelyn Burkell & Priscilla M. Regan, *Voter Preferences, Voter Manipulation, Voter Analytics: Policy Options for Less Surveillance and More Autonomy*, 8 INTERNET POL'Y REV. 4 (2019).

[29] Balkin, *supra* note 4.

control of the users' experience involves an analysis of all that the user has done based on information about that user and inferences drawn based on that information. As pointed out in Senator Warner's draft white paper, "Pervasive tracking may give platforms important behavioral information on a consumer's willingness to pay or on behavioral tendencies that can be exploited to drive engagement with an app or service."[30]

The 2006 observation of Clive Humby, U.K. mathematician and architect of Tesco's Clubcard, that, "Data is the new oil . . . It's valuable, but if unrefined it cannot really be used. It . . . must be broken down, analyzed for it to have value," has been often-repeated.[31] His reference here is to data about individuals and has fueled debates about what should be done to curtail the power of companies like Facebook, Amazon, Google, and Microsoft. The *Economist* wrote in 2017:

> Such dominance has prompted calls for the tech giants to be broken up, as Standard Oil was in the early 20th century. This newspaper has argued against such drastic action in the past. Size alone is not a crime. The giants' success has benefited consumers. Few want to live without Google's search engine, Amazon's one-day delivery or Facebook's newsfeed. Nor do these firms raise the alarm when standard antitrust tests are applied. Far from gouging consumers, many of their services are free (users pay, in effect, by handing over yet more data). Take account of offline rivals, and their market shares look less worrying. And the emergence of upstarts like Snapchat suggests that new entrants can still make waves . . . . But there is cause for concern. Internet companies' control of data gives them enormous power. Old ways of thinking about competition, devised in the era of oil, look outdated in what has come to be called the "data economy." A new approach is needed.[32]

Implicit in the above is that the crux of the current problems associated with these firms is the data about individuals that they have amassed directly, indirectly, or by inference and that these firms can use to their competitive advantage in terms of both offering products and services to individuals and also undercutting business rivals. Personal data gives these firms the central

---

[30] Mark R. Warner, *Potential Policy Proposals for Regulation of Social Media and Technology Firms*, White Paper 3, https://regmedia.co.uk/2018/07/30/warner_social_media_proposal.pdf.

[31] *See* Michael Palmer, *Data is the New Oil*, https://ana.blogs.com/maestros/2006/11/data_is_the_new.html. (last visited 2020).

[32] *The World's Most Valuable Resource is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

asset that they control. As Julie Cohen similarly notes, "the data extracted from individuals plays an increasingly important role as raw material in the political economy of informational capitalism."[33]

V. SEARCH FOR APPROPRIATE POLICY REGIME

Big data resources and applications have enhanced the power of personal data in ways that have further challenged information privacy, enhanced the competitive advantage of companies who control the data, and enabled the targeting of messages to select individuals and groups. If big data resources and applications have become integral to modern life, then the organizations and transmission mechanisms that support big data take on the features of an infrastructure.[34] Scholars and policymakers are analyzing these issues and offering a number of possible solutions, but often with a focus on one of the problems such as competitive advantage, information privacy, or targeted information. Viktor Mayer-Schonberger and Kenneth Cukier recognize a more active role for government regulation to control what they call the "data barons"—"[w]e must prevent the rise of the twenty-first century robber barons who dominated America's railroads, steel manufacturing, and telegraph networks."[35] Additionally, they advocate for the use of antitrust rules to curb abusive power and ensure conditions exist to promote a competitive market for big data, a solution that Elizabeth Warren as a 2020 Democratic presidential candidate has also called for Amazon, Facebook, and Google.[36] Most recently, several state Attorney Generals have begun investigations into antitrust violations by Facebook and Google.[37] In 2014, the President's Council of Advisors on Science and Technology (herein "PCAST") suggested a policy solution similar to "trusted third party" options, which could establish and monitor privacy-preference profiles and also review new data collection and use applications to determine how they fit within each of the profiles.[38] Balkin proposed an "information fiduciaries" scheme that would require ISPs and major online

---

[33] Cohen, *Law for the Platform Economy*, *supra* note 7.

[34] DEBORAH G. JOHNSON & PRISCILLA M. REGAN, POLICY OPTIONS FOR RECONFIGURING THE MIRRORS, IN TRANSPARENCY AND SURVEILLANCE AS SOCIOTECHNICAL ACCOUNTABILITY: A HOUSE OF MIRRORS (2014).

[35] Mayer-Schonberger, *supra* note 10, at 183.

[36] Matt Stevens, *Elizabeth Warren on Breaking Up Big Tech*, N.Y. TIMES (June 26, 2019) https://www.nytimes.com/2019/06/26/us/politics/elizabeth-warren-break-up-amazon-facebook.html.

[37] Steve Lohr, *New Google and Facebook Inquiries Show Big Tech Scrutiny is Bipartisan Act*, N.Y. TIMES (Sept. 6, 2019) https://www.nytimes.com/2019/09/06/technology/attorney-generals-tech-antitrust-investigation.html.

[38] President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective*, at 37 (May 2014).

platforms to abide by terms of trust and confidence protecting users and limit what organizations can do with user data.[39] Daniel Greenwood, at the MIT Media Lab, and colleagues suggest the establishment of a "trust network" as a system of data sharing, "elegantly integrating computer and legal rules, allows automatic auditing of data use and allows individuals to change their permissions and withdraw data."[40]

In 2018, Senator Mark Warner issued a White Paper proposing a number of policy options including one to label certain services, such as Google, as "essential services," a designation that would require internet platforms to provide access to these services on "fair, reasonable and non-discriminatory" terms (hereinafter "FRAND") and prevent them from "engaging in self-dealing or preferential conduct."[41] Daniel Crane, an antitrust law professor, raises issues with enforcement of potential FRAND obligations:

> Another key issue with FRAND commitments or obligations—one not addressed in the white paper—is what institution has jurisdiction to determine when the dominant firm has failed to honor the FRAND obligation . . . . Courts are generally very bad at setting terms of dealing . . . . Regulatory agencies might take it up, but there is no agency with the obvious expertise or resources to decide what terms online platforms should have to offer third parties.[42]

To this point, Hal Singer, an antitrust economist, suggests the establishment of a new independent "Net Tribunal"[43] to police discriminatory conduct by dominant tech platforms—and potentially internet service providers. Arguing that anti-trust law does not provide an effective solution, his proposal entails:

> [A]n alternative, ex post regime patterned loosely on the tribunal used to adjudicate discrimination complaints against cable video operators pursuant to Section 616 of the Cable Television Consumer Protection and Competition Act of 1992 (herein "Cable Act"). Although that tribunal operates under the Federal Communications Commission, the proposed tribunal here could be independent, as are

---

39 Balkin, *supra* note 4.

40 Daniel Greenwood et al., *The New Deal on Data: A Framework for Institutional Controls*, PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 192, 198 (Julie Lane et al. eds., 2014).

41 Warner, *supra* note 30, at 23.

42 Asher Schechter, *Would Sen. Warner's Ambitious Plan to Regulate Social Media Giants "Ruin" the Internet—Or Save it?*, PROMARKET (August 13, 2018).

43 Singer, *supra* note 7.

> Article I courts, operating free from reversals by political appointees at federal agencies.[44]

Sabeel Rahman, at Brooklyn Law School, begins to develop a scheme to modify classic public utility regulatory tools to achieve accountability for internet platforms to meet standards of fair access and treatment, and protection of users. However, he notes the challenging choices in terms of whether to provide for institutional oversight regulation by government, private actors or some hybrid or provide for structural regulation by addressing business models and market dynamics (2018).[45]

Currently, there is no lack of suggested regulatory and legal suggestions to tackle this problem. Not surprisingly, no single suggestion seems perfectly designed to combat the complexity of *one* of the current internet issues, much less to address all three. As Singer notes, "the internet is not one thing—it is many things, and our current regulatory regimes are struggling to address that complexity."[46] There is no question that regulators are struggling and not doing very well in this struggle. The 2015 net neutrality rules were repealed in December 2017, removing FCC jurisdiction over ISPs and reclassifying them as "information services" rather than "telecommunications services."[47] In effect, this returns jurisdiction over them to the FTC, which not only has its plate full, but also only has the power to act with *ex post* authority, the power to respond primarily to egregious cases or patterns of "deceptive and unfair trade practices," and does not have the rulemaking power. Congress is currently considering proposals to broaden FTC powers, but as exemplified by a recent hearing held in late September 2018, major internet companies—including AT&T, Apple, Amazon, Google, and Twitter—support increased staff and funding for the FTC but not enhanced legal authority.[48]

In an interesting recent essay, Frank Pasquale, a law professor at the University of Maryland, portrays this modern debate as one between Jeffersonians, advocating use of antitrust laws, and Hamiltonians, advocating specific rules to curb abuses of corporate powers. The author notes:

> It will be politically difficult to "unscramble the omelet" of currently dominant firms. Authorities are wary

---

44 Singer, *supra* note 7.

45 *See generally* K. Sabeel Rahman, *Regulating Informational Infrastructure: Internet Platforms as the New Public Utilities*, 2 GEO. L. TECH. REV. 234–251 (2018).

46 Singer, *supra* note 7.

47 Restoring Internet Freedom, FED. COMM. COMM'N, FCC 17-166 (adopted Dec. 14, 2017).

48 *Examining Safeguards for Consumer Data Privacy: Hearing Before the S. Comm. on Com., Sci., and Tech.*, 115th Cong. (2018) (statement of Sen. John Thune, Chairman, S. Comm. on Com., Sci., and Tech.).

> of reversing mergers and acquisitions, even when they are obviously problematic in hindsight. While Jeffersonians may keep our digital giants from getting bigger, Hamiltonians will need to monitor the current practices of these firms and intervene when they transgress social norms.[49]

Given the partisanship in Washington, the reluctance of internet firms to succumb to regulation, and the prevailing sense that there should not be a rush to regulate but instead a need to get it "right," it is likely that debates about what actions to take will drag on for some time. Meanwhile, current practices will continue to be unchecked, intensifying concerns about privacy, competition, and misinformation. Yet again, hindsight will likely reveal that something should have been done sooner.

The hindsight revelation may be reminiscent of the proposal for a Federal Privacy Board that was included in the original version of the Privacy Act of 1974 proposed by Senator Ervin. The question of an independent privacy agency was a point of contention even before the congressional hearings. Both the Westin/Baker study[50] (1972) and the Department of Health, Education, and Welfare (HEW) advisory committee[51] (1973) recommended against the establishment of a commission—and in congressional hearings all federal agencies and many private sector organizations voiced opposition as well. Although the Senate bill provided for the establishment of a Privacy Protection Commission, the House bill did not. The final bill established a Privacy Protection Study Commission (herein "PPSC"), which concluded in its 1977 report that existing federal agencies with regulatory authority over certain areas, such as the FTC would be appropriate control mechanisms.[52] As information practices have become more sophisticated and as other countries have established such agencies, proposals to establish a privacy commission of some type in the U.S. are raised—but have never garnered significant support or serious consideration.

However, the time might be right for serious consideration of a well-designed privacy board or commission that is premised on the concept that internet actors have a duty to act as "public trustees" in their processing of personal data. This might provide an appropriate solution for a number of reasons. First, the focus is on information practices which, as argued above,

---

[49] Frank Pasquale, *Tech Platforms and the Knowledge Problem*, 2 AMERICAN AFFAIRS 14 (2018).

[50] ALAN F. WESTIN AND MICHAEL BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING, AND PRIVACY (1972).

[51] U.S. DEPT. OF HEALTH, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973).

[52] PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977).

address privacy concerns, anti-competitive potential, and misinformation spread. Second, it embraces time-honored principles of "public interest, convenience and necessity" from early communications regulation under the FCC and recognition of "essential services" operating under "fair, reasonable and non-discriminatory" terms from antitrust regulation. Third, it acknowledges the fundamental connection between privacy and trust necessary in the information economy,[53] and would move privacy principles "from procedural means of compliance for data extraction towards substantive principles to build trusted, sustainable information relationships."[54] With an emphasis on data holders as public trustees, policy discussions would shift from focusing on the negative effects of information collection and use to determining what kinds of information practices serve a public interest in an information economy.[55] Fourth, it need not, and should not, entail a static, one-size fits all, innovation-stifling approach, but permits flexibility and learning instead—especially in areas such as the use of algorithms.

The design of such an agency is without question a challenge—especially in today's anti-regulatory environment with high levels of distrust in government. The data protection agencies of Europe and the privacy commission in Canada may provide templates that can be borrowed from and modified, especially based on their experiences with what has been effective and what has not.[56] However, the policy problem the agency seeks to address is not privacy *per se*, but on controlling the private power of internet actors, a power largely premised on their collection and analysis of personal data, which has spawned three inter-related problems: privacy, anticompetitive behavior, and misinformation.

Before tackling the question of how such an agency might be designed, let me first note that my focus is on the agency, not the standards or rules that the agency would be charged to implement. As noted above, there are numerous congressional bills and congressional testimonies discussing what rules, principles, or standards should be included in legislation. However, although as Cameron Kerry points out, there is much agreement on the key principles, nonetheless, "it is a challenge to articulate these in ways that are concrete without being too prescriptive or too narrow."[57] Although the

---

53 Regan, *supra* note 10; Richards & Woodward, *supra* note 3; Hirsch, *supra* note 25.

54 Richards & Woodward, *supra* note 3.

55 Regan, *supra* note 10.

56 *See* Colin J. Bennett & Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, Hampshire: Ashgate (2003); and, DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES (1989).

57 Cameron F. Kerry, *Will this new Congress be the one to pass data privacy legislation?*, BROOKINGS: TECHTANK (Jan. 7, 2019),

question of standards or principles is not my focus, as noted above, the shortcomings of the FIPPs approach requires a shift in policy thinking to obligate organizations to responsibly handle personal information. In setting such obligations or duties, it is first important to point out that the target of inquiry here is large organizational entities, or the "data barons" if you will, and not small, local organizations that have information on a limited number of customers or members with whom they have a direct and somewhat limited relationship.[58] Additionally, in setting obligations and duties, Margot Kaminski's conclusion that "both the current penalties and the current levels and kinds of uncertainty in the U.S. privacy regime are not enough to drive industry to the table in efficiency-maximizing ways" is important to consider.[59] She argues that effective policy will require broad standards backed by enforcement; ensuring that there is uncertainty over what the standards require and therefore driving companies to negotiate with the enforcement agency.[60] The discussion below regarding the design of a new agency assumes that Congress does pass legislation setting out broad, rather than specific, principles that would serve as a baseline for agency deliberations.

Second, this article takes the position that a new agency is needed to take the lead in these areas although it should, as will be discussed below, work with, not against, the existing agencies. At this point, a number of federal agencies exercise some jurisdiction over personal information practices in different sectors, such as the Department of Health and Human Services (HHS) over health information and Department of Education over student information. Generally, the FTC is recognized as the leading agency on privacy, but its powers in the privacy and security realm are not as extensive (for example, rulemaking power) as needed. In a fairly exhaustive analysis of FTC privacy actions, Daniel Solove and Woodward Hartzog found that FTC actions demonstrate "quite thick" jurisprudence, which has features of a "robust regulatory privacy regime."[61] As they also note, however, not all companies are required to or do have privacy policies enabling FTC jurisdiction, and FTC actions generally result in settlements,

https://www.brookings.edu/blog/techtank/2019/01/07/will-this-new-congress-be-the-one-to-pass-data-privacy-legislation/.

[58] California's CCPA excludes companies with less than $25 million in annual gross income and Senator Wyden's proposed Consumer Data Privacy Act does not cover businesses below a certain size—less than $50 million in average annual receipts and not collecting information on over 1 million people and devices. *See* Chander, *supra* note 22, fn.189.

[59] Margot E. Kaminski, *When the Default is No Penalty: Negotiating Privacy at the NTIA*, 94 DEN. L. REV. 925, 946 (2016).

[60] *Id*.

[61] Daniel Solove and Woodward Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 583–86 (2014).

which do not always generate an open record.[62] They conclude their analysis by saying that, "the FTC has not fully exerted its powers or pushed the logical ex-tensions of its theories" and could expand its powers beyond privacy policies.[63] In a subsequent article, they similarly point to the nimbleness of the FTC, its tradition of working well with other agencies with overlapping mandates, and its ability to be flexible in determining harms, but fault it for being "quite conservative" and "more of a norm-codifier than norm-maker"[64] and ask it to be "bolder and more aggressive[.]"[65]

Moreover, a new agency would not only be better positioned to counter the weaknesses of the FTC but would also better address the range of concerns about information flows that lead not only to privacy and security issues, but also unfair competition and disinformation on the internet. Additionally, its orientation would be broader than legal, allowing it to be nimbler than the FTC. Lastly, and perhaps most importantly, the FTC was founded in 1914 and designed for the problems of an earlier age—its mission, organizational culture, and statute have adapted somewhat to the challenges of the information age.[66] But at the same time, there is arguably a historical drag, a tendency towards following standard operating procedures, and a legalistic culture that constrains its ability to approach the complexity of the problems of the information age with a fresh perspective.

VI. DESIGNING A TRUST AGENCY

There are several inter-related features that are likely to be critical both to support for an agency charged with regulating internet actors so that they act as trustees of the public interest and to the success of an agency in achieving this goal. The first two involve the name and position of the agency in the federal structure, and the following five directly address designing the agency to avoid capture by regulated industries and over-politicization by partisan interests.

The first is the *name* of the agency. The policy goal to which the agency is to be committed is to require large internet actors to act as public trustees, and the *name* of the agency should reflect that—possibly the "Data Trustee Board" or the "Data Trust and Integrity Board." In this sense, it should be framed more like the National Institute of Standards and Technology (herein "NIST"), which ensures the technical integrity of the internet, but with a

62 *Id.*

63 *Id*. at 666.

64 Woodward Hartzog & Daniel Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2266 (2015).

65 *Id*. at 2234.

66 *See generally* CHRIS JAY HOOFNAGLE, FED. TRADE COMM'N PRIVACY LAW AND POLICY (Cambridge University Press, 2016) (2016).

focus on the internet's data integrity. Privacy is one—albeit, critically important—aspect of data integrity, but experience has demonstrated that privacy has not provided a compelling narrative that the public truly embraces, as it can be undermined by simplified notions of "having nothing to hide," and privacy is a multi-faceted concept that encompasses several important interests that may be under-appreciated by grouping them under privacy. The agency title should both better convey the policy goal being protected and should take advantage of the opportunity to reframe the policy issue.

The second is the *placement* of the agency in the federal organizational structure. At this point, there are a number of agencies that share jurisdiction over pieces of the three issues involving personal information flows that are examined in this paper—privacy intrusions, anti-competitive behavior, and misinformation or "fake news." Given the range of issues, the technical sophistication of information practices, and the desire to move beyond a legalistic framework, one option might be to house the new agency as a separate agency in the Department of Commerce, along with NIST and NTIA.

Given the past success of large internet actors to lobby successfully against any form of government regulation and the expertise that internet actors have over the dynamics of the flows of personal information, the primary design challenge in establishing this agency is to provide it with the institutional capacity to *avoid being captured* by the industries it is to regulate and to *insulate it from becoming politicized* while also *empowering it to collaborate* with those industries. This is no small task, but much has been written in both administrative law and political science about regulatory capture that offers some guidance in this area; however, the dynamics of capture will be contextual varying in the structure of the interest group environment and the partisan positions on regulation. Put most simply, "capture describes situations where organized interest groups successfully act to vindicate their goals through government policy at the expense of the public interest."[67] Scott Hempling points out that regulatory capture is neither corruption nor control but is essentially an attitude on the part of the regulated entities where the regulators are biased or constantly persuaded by the identity or position of the regulated rather than the merits of any arguments about the need or contours of regulation, which becomes "reflected in a surplus of passivity and reactivity, and a deficit of curiosity

[67] Michael A. Livermore and Richard L. Revesz, *Regulatory Review, Capture, and Agency Inaction*, 101 GEO. L.J. 1337, 1340 (2013); Ryan Bubb & Patrick L. Warren, *Optimal Agency Bias and Regulatory Review* 38 (New York Univ. Sch. of Law Pub. Law & Legal Theory Research Paper Series, Working Paper No. 12-47, 2013).

and creativity."[68] He goes on to argue that,

> [A]n agency is susceptible to capture when there are: (a) policy voids instead of vision; (b) priorities and procedures that reflect parties' requests rather than public interest needs; (c) chronic resource differentials between the regulator and regulated; and (d) fair-weather politicians whose support for regulation sags when pressured by those who would weaken it.[69]

David Freeman Engstrom differentiates two types of capture, both of which are likely to bedevil regulation of internet actors. The first, materialist, or classic, captures that which involves asymmetric stakes among groups, collective action problems, and structural problems. Second, a newer, non-materialist, view of capture entailing dominance of ideas that "what is good for Wall Street is good for America."[70]

Given the largely self-regulatory stance that the government has taken to this point regarding internet actors and the scale and complexity of their business models, the mandate of an independent agency in this area should not be to oversee that organizations are abiding by detailed rules and to mete out punishment. Instead, its mandate should be to work somewhat more collaboratively with internet actors to understand the goals of personal data practices, to identify consequences (intended and unintended) of those practices, and to evaluate whether the practices are consistent with the "public interest, convenience and necessity." Its mandate should not be to stifle innovation, but to ensure socially responsible innovation. Lessons and insights from co-regulation attempts in the U.S. and Europe offer some guidance as to what to avoid and what to add[71] so that an agency will need to have sufficient authority and stature to require an internet actor to modify or cease a data practice that is not in the public interest.

So, how might an agency be designed to avoid being captured or politicized while at the same time being able to maintain a collaborative relationship with the regulated industries and the trust of the public? These goals are somewhat overlapping in that features of institutional structures and capacities can address more than one goal. The key design challenges

---

[68] Scott Hempling, *Regulatory Capture*, 1 EMORY CORP. GOVERNANCE & ACCOUNTABILITY REV. 23, 25 (2014).

[69] *Id.* at 33.

[70] David Freeman Engstrom, *Corralling Capture*, 36 HARV. J.L. & PUB. POL'Y 31, 32 (2013)

[71] *See generally* Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439, 480 (2011); Dennis D. Hirsch, *Going Dutch? Collaborative Dutch Privacy Regulation and the Lessons It Holds for U.S. Privacy Law*, 2013 MICH. ST. L. REV. 83, 166 (2013); David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. 329, 377 (2014).

include decisions about: (1) whether the agency should have a single or multi-member head, the length of terms of service, and the conditions under which the head(s) of agencies can be removed; (2) what is the funding source for the agency; (3) how can the agency marshal the expertise that it needs to regulate; (4) what are the relationships of the agency with other federal agencies, as well as state actors and public advocates; (5) how transparent is the decision-making of the agency; and (6) what is the ability of the agency to generate the information it needs to regulate effectively?

A. Agency Leadership

There are advantages as well as disadvantages to both single member and multi-member agency leadership.[72] Single member heads, particularly with longer terms of service (five to seven years, for example) provide a clear point of authority, enabling the agency to act quickly and decisively, and some insulation from the politics of the day, as well as providing a single point of accountability to the public. At the same time, single member heads arguably have too much independent authority. Multi-member heads with overlapping terms of service generally entail different perspectives and involve a certain amount of bargaining, negotiating, and compromise to reach decisions, thus providing a type of internal check and balance. The Consumer Financial Protection Board (herein "CFPB") and the Federal Housing Financial Agency (herein "FHFA"), both of which were established in the wake of the 2008 financial crisis, are single-member heads with five year terms with Presidential removal only for cause (e.g., inefficiency, neglect of duty, or malfeasance). However, the constitutionality of single member heads for both the CFPB and FHFA has been challenged on the basis that it entails too much independence from political control, especially when combined with a source of funding independent of the appropriations process.[73] Given this constitutional uncertainty, it is likely wise to establish a multi-member leadership structure with overlapping five-year terms and removal only for well-defined cause, with some combination of congressional and presidential appointment.

B. Funding Source

Given the vast financial resources of major internet actors and the lack of detailed information about their business models, an independent source

[72] *See generally* Kirti Datla & Richard L. Revesz, *Deconstructing Independent Agencies (and Executive Agencies)*, 98 CORNELL. L. REV. 769 (2013).

[73] Sarah Harrington, *Kavanaugh on the Executive Branch: PHH Corp. v. Consumer Financial Protection Bureau*, SCOTUS BLOG (August 8, 2018, 10:25 AM), https://www.scotusblog.com/2018/08/kavanaugh-on-the-executive-branch-phh-corp-v-consumer-financial-protection-bureau/.

of funding for this new agency seems to be a critical factor in ensuring that the agency would avoid both capture and politicization. There are two ways to ensure some financial independence for an agency. The first is to enable agencies to submit their budget proposals directly to Congress bypassing OMB; this eliminates the executive's ability to change the agency's request, but still leaves it open to congressional wrangling. The second, and more effective alternative, is to provide agencies with an independent source of funding, such as by requiring the regulated entities to pay mandatory fees to the agency. As Rachel Barkow points out, the Federal Reserve's funding is through assessments on member banks, and the Office of Thrift Supervision, the Office of the Comptroller of the Currency, and CFPB are similarly funded; this insulates the agencies from both congressional and presidential influence.[74] Charles Kruly similarly points that "when Congress combines self-funding with other traditional indicia of agency independence—typically, structural features that insulate an agency from executive control—Congress creates what are likely the most structurally independent agencies in the federal government;"[75] however, he goes on to note the importance of other structural features in ensuring this independence.

C. Expertise

Providing the agency with a level of expertise so that it can evaluate what the industries say is also critical to maintaining independence and avoiding capture and politicization. This can be achieved both at the leadership level and at the staff level. In this case, the leadership and staff of the agency should also be interdisciplinary and include, for example, technologists, data scientists, ethicists, and social scientists, with lawyers kept to a minimum. Presidential or congressional appointees can be required to have certain qualifications, which then somewhat mitigates partisan influence. This is not an unusual requirement for agencies where scientific or technical expertise is important—for example, by statute, the leadership of the Food and Drug Administration requires scientific expertise, the Defense Nuclear Facilities Safety Board requires "respected experts in the field of nuclear safety," the Commissioner of the Consumer Product Safety Board cannot hold the office of Commissioner if he or she is "in the employ of, or holding any official relation to, any person engaged in selling or manufacturing consumer products" or owns "stock or bonds of substantial value in a person so engaged" or "is in any other manner pecuniarily

[74] Rachel E. Barkow, *Insulating Agencies: Avoiding Capture Through Institutional Design*, 89 TEXAS L. REV. 15, 44 (2010).

[75] Charles Kruly, *Self-Funding and Agency Independence*, 81 GEO. WASH. L. REV. 1733, 1736 (2013).

interested in such a person."[76] Similar requirements can be established for staff. Initially, it may also be wise to detail staff from other federal agencies with jurisdiction in this area, such as the FTC, FCC and NTIA, which would transfer not only a degree of expertise but also some measure of institutional memory to the new agency.

D. Relationships with Federal, State, and Public Actors

This brings us to the question of the relationships of the new agency with other federal agencies, as well as state actors and public advocates. The issues of online privacy, net neutrality, and online speech have spawned a cottage industry of potential and actual regulators, as well as a range of industry and public interest groups. This is already a crowded field, with the FTC, FCC, and NTIA, as well as Department of Education and HHS, already having some jurisdiction, but as the earlier analysis indicates the field is not one where there is clear leadership and one where there is need for more coordination and authority to act. Rather than resist the existing governmental actors in this area, a new agency could utilize their support, working collaboratively with these agencies. But, as Rachel Barkow argues, the new agency would need to be defined as having primary responsibility:

> It is all too easy for agencies to point fingers at each other with no one ultimately held accountable. Indeed, that scenario is eerily similar to the lead-up to the recent financial crisis, with each over-lapping regulatory agency essentially casting blame on others. To remedy this risk and achieve a check on capture, the insulated agency should be designated as the primary enforcer to ensure greater accountability and to increase the incentives for the responsible agency to take action.[77]

Designating the new agency as primary is likely to generate opposition from the large internet actors, who at this point are quite comfortable with having the FTC as the primary agency in this area and are supportive of more staff for the FTC, but not more enforcement power. However, indicating the new agency as the primary agency is critical to its effectiveness. The new agency's relationships with state actors are likely to be easier to navigate. As Barkow points out in guidance on how to design institutions to avoid capture, allowing state Attorneys General (AG) to also bring enforcement actions can be an effective check against capture and protects against underenforcement of regulations. AG involvement provides an additional level of protection against the possibility that federal agencies bow to the

[76] Barkow, *supra* note 74, at 48.
[77] Barkow, *supra* note 74, at 56.

President's priorities, which may be dictated by powerful interest groups.[78] Professor Danielle Citron has carefully documented the activities of AGs in privacy and security issues and concludes that they have responded quickly to consumer privacy concerns in part because they are less constrained by "bureaucratic wrangling."[79] Citron also notes that AGs have institutionalized collaboration about best practices and emerging risks in the monthly telephone calls of the NAAG Privacy Working Group.[80] A new agency would also be able to work with this Group on a regular basis.

Institutionalizing collaboration with public advocates is another design feature to avoid capture and over-politicization. There are a range of public interest groups, including most prominently the ACLU, CDT, EPIC, and EFF, that are concerned with privacy and security, anti-competitive behavior of internet actors, net neutrality, and disinformation on the internet. There are a number of ways that these groups might be formally, as well as informally, involved in a new agency's activities. Examples might include membership on an advisory committee that meets regularly or a formal position of public advocate to represent "the public's interest before the agency."[81] Additionally, the new agency might institutionalize a similar type of involvement for privacy professionals "on the ground" and for the International Association of Privacy Professionals (IAPP).[82] The richness and robustness of the interest groups in this area should be an asset for the new agency. Further, institutionalizing collaboration with these groups is an important buffer against industry capture and over-politicization.

E. Transparency and Information Generation

Given that the mandate of the new agency is to act as a public trustee, maintaining the transparency of the agency's work is a priority and is also a protection against capture and politicization. As Barkow argues:

> [O]ne of the most powerful weapons policy makers can give agencies is the ability to generate and disseminate information that is politically powerful . . . . The key is to give the agency the authority to study and publicize data that will be of interest to the public and help energize the public to overcome collective action problems and rally behind the

---

78 *See* Barkow, *supra* note 74, at 57–58.

79 Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 786 (2016).

80 *Id.* at 790.

81 *See* Barkow, *supra* note 74, at 62.

82 *See generally* Kenneth A. Bamberger & Deirdre Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2010).

agency.[83]

Policy and decision processes of the agency should be open to the public utilizing traditional Administrative Procedure Act (APA) practices regarding notice and comment periods for proposed regulations. As Engstrom points out, the transparency and pluralistic participation required by rulemaking is more insulated from regulated interest group influence and bolsters congressional oversight by providing "fire alarms,"[84] using a distinction developed by McCubbins and Schwartz.[85] Consistent with this, proposed regulations should not be subject to review by OMB's Office of Information and Regulatory Affairs (OIRA) providing protection against both capture and politicization. Likewise, decisions regarding industry practices that allegedly violate information practice regulations should be made publicly available.

Two additional design features can enhance traditional agency transparency requirements. The first, as Barkow suggests, is the establishment of a research arm within agencies—an idea that is very suitable in this instance, especially in the area of big data and algorithms.[86] This is consistent with Orley Lobel's argument that, in dealing with regulation of platforms, "regulatory agencies should view themselves not merely as reactive enforcers, but also as active researchers of these changes."[87] Another design feature is the utilization of third-party auditors, which also would provide a means of gaining information about how internet actors are using algorithms. As Lesley McAllister explains, "private third-party verifiers essentially act in the place of governmental agents to conduct inspections and make regulatory compliance determinations. Governmental agencies, in turn, take on new roles in coordinating and overseeing these private actors. As a form of public-private governance, third-party verification may further the goals of social regulation."[88] Although this may reduce the direct costs to a government agency, it establishes a longer chain of accountability and requires careful oversight both of the third-party verifiers and the industry. It has the advantage, however, of providing a means to extract relevant information.

---

[83] Barkow, *supra* note 74, at 59.

[84] David Freeman Engstrom, *Corralling Capture*, 36 HARV. J. L. PUB. POL'Y 31, 35–36 (2013).

[85] *See* Matthew D. McCubbins & Thomas Schwartz, *Congressional Oversight Overlooked: Police Patrols versus Fire Alarms*, 28 AM. J. POL. SCI. 165, 166 (1984).

[86] Barkow, *supra* note 74, at 60.

[87] Orly Lobel, *Law of the Platform*, 101 MINN. L. REV. 87, 163 (2016).

[88] Lesley K. McAllister, *Regulation by Third-party Verification*, 53 B.C. L. REV. 1, 12 (2012).

VI. CONCLUSION

In the wake of the Facebook/Cambridge Analytica debacle, somewhat bizarre censoring actions on the part of social media companies leading up to the mid-term elections, heightened public concern about algorithmic decision-making, and increased concentration among major internet actors. There may actually be a window to engage the complexity of controlling the private power of major internet actors rather than endorse incremental policy changes that are destined to be ineffective. Until now, as Julie Cohen aptly puts it, "Law for the platform economy is already being written—not via discrete, purposive changes, but rather via the ordinary, uncoordinated but self-interested efforts of information-economy participants and the lawyers and lobbyists they employ."[89] Much of the congressional debate, as well as the public debate, has coalesced around proposals to strengthen the role of the FTC and to provide more effective "notice and choice" to consumers—both of which fail to understand the larger economic changes that have taken place in the platform-based economy and the dominance of large internet actors.

In this paper, I have advanced two related arguments. The first is that the current unchecked flows of personal information have not only caused privacy and security problems but have also played pivotal roles in causing fake news and misinformation and increasing the power of major internet platforms. If policy addresses this underlying cause effectively, then such policy would not only address information privacy issues, but also ameliorate or mitigate the issues associated with anti-competitive behavior by ISPs and internet platforms, and with misinformation and fake news. My second argument is that the effectiveness of policy in this area hinges on the establishment of a new agency designed to avoid capture by the regulated industries and over-politicization by partisan interests.

89 Cohen, *Law for the Platform Economy*, *supra* note 7, at 136.