Duke Law Journal Online

VOLUME 65 FEBRUARY 2016

RESPONSE TO *PRIVACY AS A PUBLIC GOOD*

PRISCILLA M. REGAN†

INTRODUCTION

Most of the legal, philosophical, and social-science thinking about privacy emphasizes its value to the individual with less attention to its value to society. Professors Fairfield and Engel join a growing number of privacy scholars who are probing privacy's value to society and policy options to protect privacy's social value.[1] They signal its social importance and also underscore weaknesses in current policies designed to protect privacy: "Inattention to privacy's public-good nature has led privacy policy astray."[2] They seek to explain how, and why, informed individuals who highly value privacy act in ways that reduce the privacy of others and of society. They explore how to help "promote collective action on privacy"[3] in order to avoid or to remedy what they appropriately refer to as a "social dilemma."[4]

Applying behavioral economics to identify new approaches to privacy protection, they recommend four primary changes in approach: 1) a focus on empowering groups; 2) leveraging inequity aversion, reciprocity, and normativity to lessen exploitation among group members; 3) positive framing to promote altruism; and 4) communication and sanction as key components of group

† Professor, School of Policy, Government, and International Affairs, George Mason University.

1. *See* Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385 (2015); *see generally* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES (Beate Roessler & Dorota Mokrosinska eds., 2015).

2. Fairfield & Engel, *supra* note 1, at 392.

3. *Id.* at 393.

4. *Id.* at 392.

coordination.[5] Behavioral economics' view that individuals do not behave rationally with respect to privacy protection is widely supported by evidence.[6] People do not read privacy notices, decline frequent-shopping programs, clear their online cookies, turn off their cell phone location tracking, or adopt any one of a myriad of options available to them to protect privacy. Much of the research in this area concludes that there is indeed a "privacy paradox"[7] as individuals disclose personal information, despite their expressed interests in privacy.

Behavioral economists suggest that this is not at all surprising, given some uncertainty about risks and/or rewards. People discount or devalue the future; therefore, privacy harms or invasions are not likely to immediately result from an action or inaction, but, instead, will, or will not, occur at a later time. In this sense, protecting privacy is like exercising, dieting, or saving for retirement—people may realize it is a good idea, but the incentive system allows, indeed encourages, them to put it off until a later date. Moreover, the privacy implications of action, or inaction, are secondary to the primary activity; for example, people are focused on the online transaction of buying a book, not on how that activity may implicate their privacy. With the advent of both online social networking and big data mining, these individual privacy calculations affect not only the individual herself but also others.

Overall, I applaud the efforts of Fairfield and Engel to move forward the conversation on privacy as a public good, and to investigate the insights and directions behavioral economics might contribute to this conversation. In this response, I will address four issues raised by their analysis. I do this in the spirit of moving this line of thinking forward, as I agree with the authors on the need for "more extensive study of privacy as a public good"[8] and their wish "not to settle a debate, but to spur further inquiry."[9] Part I will examine their depictions of individuals in groups to gain a better sense of what is still to be explored to more fully understand the relationships that are

5. *Id.* at 448–56.

6. *See, e.g.*, Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509 (2015).

7. Susan B. Barnes, *A Privacy Paradox: Social Networking in the United States*, 11 FIRST MONDAY (Sept. 2006), http://firstmonday.org/article/view/1394/1312 [http://perma.cc/N6PQ-K3SL].

8. Fairfield & Engel, *supra* note 1, at 393.

9. *Id.* at 457.

in play here. Part II will explore their focus on the "group" and suggest some ways in which it might be important to further clarify this concept. Part III will explain why I believe the platform on which groups exist and interact needs a more central place in our analysis of privacy as a public good. Part IV will address whether Fairfield and Engel's preference for policy tools that do not rely on "government intervention"[10] constrains the analysis needed to explore ways to protect privacy as a public good. This part will also examine the failure to recognize the government intervention involved in some of the policy tools they do recommend. Each of these points is developed briefly below, but each is also in need of further data collection and analysis.

I. INDIVIDUALS IN GROUPS

Fairfield and Engel are interested in identifying tools that groups can use to sustain the production of public goods and that might also be employed to sustain privacy as a public good. Their focus, and their language, however, seems to alternate between "groups" as stand-alone entities and 'individuals in groups' or 'members of groups.' They persuasively make the case that individual-focused privacy approaches negatively impact others, are not effective even from an individual perspective, and have reached diminishing returns. Examining ways to empower groups in the face of what is in reality a social dilemma offers a compelling path for analysis. Clarity and consistency, however, about whether the goal is to empower "groups" as the unit of analysis or "individuals in groups" is necessary. I believe that despite the authors' claim that "[t]he relevant privacy unit is the group, rather than the individual,"[11] the unit on which their analysis actually concentrates is "individuals in groups."

This modification in emphasis raises the question of whether one can understand and operationalize an analysis based on "groups" without probing how individuals in groups differ from individuals acting individually. In other words, we might assume that individuals acting as individuals do so based on their calculation of their self-interest, however accurate or flawed that might be. Individuals in groups are possibly making a different calculation in that they take into account not only their own interest as a member of the group,

10. *Id.* at 396.

11. *Id.* at 456.

but also the likely interests and behavior of others in the group. The authors argue that "groups and individuals have different incentives,"[12] and that

> [i]ndividuals who face the social dilemma of privacy face three strong pressures to defect even if they are inclined to cooperate: they realize that their individual efforts will only cost them; that others will likewise defect over time; and that the development of technology tends toward ever-greater intrusions on privacy.[13]

The result is that "the generosity of volunteers with respect to their personal data creates a system that almost exclusively impacts others."[14]

The focus on individuals acting as members of groups and not merely as isolated individuals adds a valuable dimension to our understanding of privacy actions and inactions. If this is indeed the case, then a key dilemma or problem is to make it possible for individuals to realize that they are members of groups and that their actions affect not only themselves but also others in their groups. As Fairfield and Engel elaborate the argument that privacy is a public good, they reiterate that "[i]n weighing important decisions about privacy, individual and group incentives diverge. And without measured intervention, individuals' fully informed privacy decisions tend to reduce overall privacy, even if everyone cherishes privacy equally and intensely."[15] Individuals do not recognize that the sum of the potential damage from one's own and others' disclosures results in a social balance that is negative.[16]

The objective then becomes how to get individuals to realize that their individual behavior affects not only themselves but others as well—and in some cases others whom they care about deeply, for example, family members. This is an important refocusing for the discussion of privacy and for the development of options for protecting privacy. As privacy scholars move in this direction, we should draw upon the insights of sociologists[17] and social

12. *Id.* at 400.

13. *Id.* at 433

14. *Id.* at 406.

15. *Id.* at 423.

16. *See id.* at 396–421 (describing the negative externalities associated with information disclosure).

17. *See generally, e.g.*, IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL SPACE, TERRITORY, AND CROWDING (1976).

psychologists,[18] as well as communication scholars,[19] to better understand individual behavior in groups. The research on privacy behavior on social-networking sites provides some valuable applications of the insights of sociologists, social psychologists, and communication scholars. The current policy focus on individual control "complicates group efforts to maintain coordination in the face of a social dilemma."[20] As Fairfield and Engel point out, it is therefore necessary to shift the focus from empowering individuals to improving group coordination[21] so that groups are empowered to resist privacy's social dilemma.[22] To achieve this it seems necessary not only that individuals in groups are given the means to coordinate in ways consistent with such ends, but also that "the social and systemic harms caused by the collection, aggregation, and exploitation of data"[23] are recognized by the law.

II. TYPES OF GROUPS

As we move the analysis to improving group coordination, it becomes necessary to differentiate groups. Fairfield and Engel analyze two group characteristics that they think are relevant to the online privacy debate: first, size, which they conclude does not alone disqualify groups from cooperating on better privacy outcomes;[24] and second, player heterogeneity and conditional cooperation.[25] Based on their analysis of both characteristics, Fairfield and Engel conclude that neither of these is determinative but both play a role. They deduce that "[s]mall, tightly nested groups" will find it easier to cooperate and receive more from cooperating with one another,[26] and that "one is more likely to cooperate in an environment in which each

18. *See generally, e.g.*, Jacquelyn Burkell & Alexandre Fortier, *Privacy Policy Disclosures of Behavioural Tracking on Consumer Health Websites*, 50 PROC. AM. SOC'Y. INFO. SCI. & TECH. 1 (2013) (describing privacy-policy challenges in the context of consumer-health information).

19. *See generally, e.g.*, SANDRA PETRONIO, BOUNDARIES OF PRIVACY: DIALECTICS OF DISCLOSURE (2002).

20. Fairfield & Engel, *supra* note 1, at 411.

21. *Id.*

22. *See id.* at 413–14 (describing the traditional focus on individuals, and the need for a focus on groups).

23. *Id.* at 425.

24. *Id.* at 441–44.

25. *Id.* at 444–48.

26. *Id.* at 443.

person is perceived to benefit from privacy equally."[27] The universe of online groups that fall within these two parameters, however, is likely to be somewhat limited, and the examination of other group characteristics, as well as the interactions among these, will require further research and analysis.

In terms of group characteristics that are likely to affect the groups' aptitude for cooperating on privacy, three appear to be important: the context of the group, its internal dynamics, and the age of its members. Helen Nissenbaum's framework of contextual integrity provides a logical dimension to explore the capacity and inclination of a group to cooperate to protect privacy.[28] For example, book clubs for mystery readers are less likely to share similar norms about privacy and more likely to find this context less critical to their overall privacy than support groups for those with a terminal disease. Those who share a professional identity are likely to fall somewhere in between the two. Context here may provide an umbrella concept for a number of group characteristics which sociologists distinguish—such as sense of unity, common goals, similar behavior, and reciprocal relations. But context also draws attention to the notion of shared-informational norms, which, as Nissenbaum states, "define and sustain essential activities and key relationships and interests, protect people and groups against harm, and balance the distribution of power."[29]

The internal dynamics of a group are also likely to be relevant to achieving cooperation. Close-knit groups may initially be seen as more likely to be able to cooperate and protect privacy. Such groups share a common goal, generally know each other rather well, interact frequently, and have developed some understanding of group members. At the same time, the internal dynamics of such a group are likely to affect the group's capacity to coordinate on privacy protection. In this sense, such groups may be like families—functional or dysfunctional in their own idiosyncratic ways—or cliques with their own power dynamics. These peculiarities are likely to play out in ways that may not be particularly privacy friendly, as information about other members in the group, especially potentially

27. *Id.* at 446.

28. *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010).

29. *Id.* at 3.

embarrassing information, is often used by others to leverage influence or control within the group itself.

Interestingly, the age of group members may also affect the group's ability to cooperate and protect privacy. Despite common perceptions that young people do not care about privacy and share everything online, empirical studies demonstrate that they do care about privacy and take actions to shield information in different ways.[30] Young people interact with their online communities in quite complex ways and for a variety of purposes including personal identity formation, strengthening of friendships, developing of a range of skills and competencies, self-presentation, and identity play.[31] Young people do not regard privacy and publicity as a zero-sum game but instead as "co-created through social interactions; both privacy and publicity coexist in a dynamic negotiation of boundary setting that seeks to manage a multiplicity of revelations and a multiplicity of audiences."[32]

The discussion of groups above highlights their variety and complexity, leading to the conclusion that not all groups are equal, and raising the question of whether the tools for coordination and communication can operate similarly across groups. In developing a typology of group characteristics to differentiate the ability of group members to cooperate to achieve more privacy for the group as a

---

30. *See* eGIRLS, eCITIZENS (Jane Bailey & Valerie Steeves eds., 2015); VALERIE STEEVES, YOUNG CANADIANS IN A WIRED WORLD, PHASE III: TRENDS AND RECOMMENDATIONS (2014) (ebook), http://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/full/YCWWIII_Life_Online_FullReport.pdf [http://perma.cc/AS5X-VNNY]; Sonia Livingstone, *Mediating the Public/Private Boundary at Home: Children's Use of the Internet for Privacy and Participation*, 6 J. MEDIA PRAC. 41 (2005); Susan B. Barnes, *A Privacy Paradox: Social Networking in the United States*, 11 FIRST MONDAY (Sept. 4, 2006), http://www.firstmonday.org/article/view/1394/1312 [http://perma.cc/44G5-8K7A]; danah boyd & Alice E. Marwick, *Social Privacy in Networked Publics: Teens' Attitudes, Practices and Strategies* (unpublished paper presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society") (Sept. 22, 2011), http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1925128_code1210838.pdf?abstractid=1925128&mirid=1 [http://perma.cc/DQ6J-R2NL].

31. *See generally* Sonia Livingstone, *Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-Expression*, 10 NEW MEDIA & SOC'Y 393 (2008); Leslie Shade, *Internet Social Networking in Young Women's Everyday Lives: Some Insights from Focus Groups*, OUR SCHS. / OUR SELVES, Summer 2008, at 65; Patti M. Valkenburg & Jochen Peter, *Preadolescents' and Adolescents' Online Communication and Their Closeness to Friends*, 43 DEVELOPMENTAL PSYCHOL. 267 (2007).

32. Valerie Steeves & Priscilla Regan, *Young People Online and the Social Value of Privacy*, 12 J. INFO., COMM. & ETHICS SOC'Y 298, 302 (2014).

whole, Sandra Petronio's Communication Privacy Management (CPM) framework is relevant: "CPM proposes that initial disclosures set into motion a need for boundary coordination because there is an expected guardianship of the information often assumed by both the discloser and the recipient."[33] She proposes five types of decision criteria that are used in the development of privacy rules: cultural, gendered, motivational, contextual, and risk-benefit.[34] She also suggests that individuals set these boundaries differently depending on the stage of their lives (child, adolescent, adult, and elderly).[35]

The complexity of groups also raises the question of whether "group" is the correct term to employ in these discussions or whether "social network" more appropriately captures reality. Social network provides a more fluid sense of today's relationships as well as a focus on both the flow of information and the pivotal role of particular individuals or nodes within the network. It also highlights the overlapping nature of these types of relationships. Lior Jacob Strahilevitz suggests four factors, all quite similar to those identified above for groups, that affect how information will be disseminated in a network: the structure of the network, including whether there are weak ties or strong ties; the presence or absence of supernodes; cultural variables, such as existence of legal or social norms and knowledge of values of others in the network; and the nature of the information itself, including whether it is timely, complex, and likely to degrade or endure.[36] Similarly, Alice Marwick and danah boyd view the current information and cultural landscape as creating "networked publics" and necessitating a conceptualization of privacy that moves "from an individualistic frame to one that is networked."[37]

III. PLATFORM ON WHICH GROUPS OPERATE

The reality is that most of the groups of interest to Fairfield and Engel are online groups and most online groups are not self-forming, self-organizing, or self-governing entities, and thus are not in total

33. PETRONIO, *supra* note 19, at 11.

34. *Id.* at 24–26.

35. *Id.* at 26–27.

36. Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy* 22–45 (U. Chi. Law Sch., John M. Olin Law & Econs. Paper No. 230, 2004), http://www.law.uchicago.edu/files/files/230-ljs-privacy.pdf [http://perma.cc/HL8U-9UAB].

37. Alice E. Marwick & danah boyd, *Networked Privacy: How Teenagers Negotiate Context in Social Media*, 16 NEW MEDIA & SOC'Y 1051, 1052 (2014).

control of their rules and possibilities. The architecture of a site shapes the group and sets the rules. The architecture and rules are determined by the business model of the social networking site, not by the interests of the users or groups on the site. The ability of the group to control privacy is constrained and determined by what the social network or online platform permits. Privacy defaults, system architecture, nested systems—basically as Lawrence Lessig pointed out early in these debates, "code"[38]—are determinative not only of privacy possibilities and options but also of a group's prospects for coordinating and communicating. In order to seriously consider the potential effectiveness of coordination and collaboration among members of groups on social networking sites, we need a more complete and realistic understanding of how the platform on which a group operates constrains both how much a group can empower itself to better coordinate and also how much a group can be empowered.

For example, I recently received an RSVP for a professional event on Eventbrite and was asked if I wanted to see whether anyone else I knew responded that they were coming—the website being willing to share with me information that others might not realize would be shared, as well as providing incentives for me to attend (or possibly not attend) depending on who else was attending. Similarly, Instagram suggests people whom I should follow; this occurs not at the initiative of those people, but at Instagram's analysis of who in my "group" is following whom. And Google recommends whom I should add to my circles or my Google+, informing me of "who I may know." Fairfield and Engel note the reality of such interconnections: "Engaging with social media is . . . not an individual choice. It is an inevitable outcome of being in almost any social situation."[39] But what occurs online seems far less "inevitable" and far more structured by the platforms and interests of the social-media in question. Under these circumstances, the social media platform is organizing the group, not the group members. How then can group members communicate and coordinate to protect their shared interest in privacy unless the social media platform cedes control to the group members?

The type of control necessary to achieve the degree of communication and coordination that Fairfield and Engel propose is not provided by current privacy notices and settings, or by standard

38. *See generally* LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE (1999).

39. Fairfield & Engel, *supra* note 1, at 402.

"terms of use" agreements. For example, Facebook's Data Policy states:

> When you use third-party apps, websites or other services that use, or are integrated with, our Services, they may receive information about what you post or share. For example, when you play a game with your Facebook friends or use the Facebook Comment or Share button on a website, the game developer or website may get information about your activities in the game or receive a comment or link that you share from their website on Facebook. In addition, when you download or use such third-party services, they can access your Public Profile, which includes your username or user ID, your age range and country/language, your list of friends, as well as any information that you share with them. Information collected by these apps, websites or integrated services is subject to their own terms and policies.[40]

Nor is such coordinating control for a group provided by privacy seals or ratings that are often unclear to users and may not be administered by the rating organization in a responsible and effective manner.[41] Fairfield and Engel's recognition of the importance of developing tools by which individuals in groups and social networks can discover in a meaningful way the information-flow implications of their decisions, as well as how those decisions affect the flow of information about others, opens an important avenue for theoretical and policy work.

What types of tools might be available for groups to cooperate, even in the environment of large social networks with their current business models? Fairfield and Engel suggest several: given the value of repeat play in fostering cooperative behavior, a "featured contact" widget to remind users of those with whom they have not interacted recently, a feature that would aggressively promote the privacy-seeking actions of others, a "like" feature for privacy-enhancing technologies, simplified terms of service, and opt-in permission for the sharing or selling of information.[42] In some instances, for example opt-in permissions, such tools have not been supported by business

40. *Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy [https://perma.cc/MB7E-ZW6Q].

41. Press Release, Fed. Trade Comm'n, TRUSTe Settles FTC Charges It Deceived Consumers Through Its Privacy Seal Program (Nov. 17, 2014), https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its [https://perma.cc/3WRE-HC88].

42. Fairfield & Engel, *supra* note 1, at 439.

and other website operators as, given the costs on the business, there is little incentive to provide them.[43] Other tools, such as the "featured contact" widget, are likely to be perceived as "creepy" by users, as the reaction to Facebook's News Feed demonstrates.[44] As Fairfield and Engel note, tools to permit users to differentiate groups are valuable and are already embedded in social networks sites where the site administrator has made them available.[45] Additional privacy enhancing technologies,[46] some types of privacy-by-design,[47] or "differential privacy"[48] provide promise for user control that could be employed for collaboration and coordination among members of groups. But also needed are more system-wide—rather than site-specific—means for differentiating spaces or places where individuals who share interests and common levels of privacy as a public good are able to organize themselves.

This might entail a categorization of different types of online spaces or places. For such a categorization to work effectively and be easily understood, it would need to be universal, not particular to one social networking platform or site. It would also need to be global, given that many online social groups cross national boundaries. Such a scheme is likely to involve Internet standards setting, governance organizations such as the World Wide Web Consortium (W3C) or the Internet Engineering Task Force (IETF), or a coordination similar to that provided by Internet Corporation for Assigned Names and Numbers (ICANN). These are all international bodies, generally non-profit rather than business or government, with some responsibility for the effective operation of the backbone and coordination of the Internet, focused on architecture, protocols, and memorandums of understanding.

---

43. *See* Priscilla M. Regan, *Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows*, 59 J. SOC. ISSUES 2, 263–82 (2003).

44. E.J. Westlake, *Friend Me if You Facebook: Generation Y and Performative Surveillance*, 52 TDR: THE DRAMA REV., Winter 2008, at 4, 21–40.

45. *See, e.g.*, *Using Twitter Lists*, TWITTER, https://support.twitter.com/articles/76460# [http://perma.cc/VR9J-H5QE].

46. Sarah Spiekermann & Lorrie Faith Cranor, *Engineering Privacy*, 35 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, Jan./Feb. 2009, at 67, 67–82.

47. *See* Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L.J. 1333, 1349–77 (2013).

48. Cynthia Dwork, *Differential Privacy: A Cryptographic Approach to Private Data Analysis*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 296, 301 (Julia Lane et al. eds., 2014).

If the Internet has now become essential to social life, then a similar backbone and architectural design for group coordination for public goods, such as privacy, might indeed be necessary. As Fairfield and Engel persuasively argue, the "public bad" of lack of privacy is

> not only a bad deal for the community of users at the time information is revealed, they potentially grow worse over time. The public bad of lack of privacy increases over time as . . . [t]echnological increases in storage capacity and in the predictive power of machine analytics undermine incentives to seek privacy.[49]

Given that the collective value, efficiency, and usefulness of the Internet is likely to be negatively impacted if the public bad of lack of privacy continues to accrue, various components, including online platforms, may begin to recognize the value of an overall coordination mechanism that would easily signal to users the privacy norms and communication tools for a particular part of that online platform. The goal here would be to make visible the privacy implications which to date have effectively remained invisible to those affected.

IV. ROLE OF GOVERNMENT

If the goal is to help "promote collective action on privacy,"[50] then another critical avenue for further research is to determine what the appropriate role of government is under particular circumstances. Fairfield and Engel recognize the difficulties of codifying stronger privacy protections and suggest that if groups were "aided in their struggle to produce public goods by institutions, such as communication, framing, or sanction . . . communities can manage public goods without heavy-handed government intervention."[51]

The authors are somewhat less clear on what kind of government intervention would be needed to aid groups in their struggle. They appear to favor tools "that permit groups to sustain cooperation and protect privacy even without direct government intervention."[52] They note that other analysts are exploring an approach to protecting privacy as a public good that is informed by environmental law and view this as a valid approach, and one well-suited for dealing with

---

49. Fairfield & Engel, *supra* note 1, at 424.
50. *Id.* at 393.
51. *Id.* at 386.
52. *Id.* at 396.

large-scale bad actors which "may be necessary to restrain mass consumer surveillance" but may not "succeed in the current political climate."[53] The path identified by Fairfield and Engel focuses instead on "the small but constant contributions that users make exposing data about one another, the prisoners in a prisoners' dilemma."[54] However, this does raise the question of whether this path is consistent with—or realistic in light of—what they describe earlier as the "hybrid corporate-government dragnet surveillance"[55] and the big data practices currently receiving more attention and traction.

At the same time, they draw a parallel with other public goods: "Clean air, safety, roads, and the common defense all share the same incentive structure."[56] But in these cases, the group rules and structural conditions are all the result of government intervention and regulation. The authors, however, do not address the question of whether self-regulation, absent government action, would actually work to achieve their desired end. I am skeptical that self-regulation would work—both because the last thirty years of a self-regulatory approach provide evidence of its limits unless the interests of the companies and the interests of the consumers are perfectly aligned, and because giving groups more ability to self-organize is not in the interests of most websites. Thus some level of regulation appears necessary to require public, private, and non-profit websites to provide rules and tools for groups to communicate, frame, and sanction.

There is growing recognition that these complex organizational systems are not only technological systems, but that they are also more fundamentally socio-technical systems.[57] In these complex systems, as Fairfield and Engel convincingly demonstrate, lack of privacy is a public bad. They note that, according to the public bad model, if "each user were to sum up the potential for damage resulting from her own and everybody else's disclosure, she would see that the social balance is negative—implying that no one would want to join a social network where the business model is based on disclosing private information."[58] Yet people do, in droves. Although

53. *Id.* at 420.

54. *Id.*

55. *Id.* at 404.

56. *Id.* at 391.

57. *See generally* DEBORAH G. JOHNSON & PRISCILLA M. REGAN, TRANSPARENCY AND SURVEILLANCE AS SOCIOTECHNICAL ACCOUNTABILITY: A HOUSE OF MIRRORS (2014).

58. Fairfield & Engel, *supra* note 1, at 424.

Fairfield and Engel wish to "focus less on large-scale offenders who are most analogous to the factories of environmental-law analysis,"[59] and more on small groups, the reality is that even small contributions are made on the platforms of the large-scale offenders and as part of an even larger integrated infrastructure of information exchanges.

Under these conditions, as I have argued elsewhere in more detail, a more active role for the government appears essential.[60] If privacy is viewed not as a private good but as a public good, then the policy question becomes how to encourage individuals as members of groups and organizational platforms on which these groups operate to take into account social benefits and social costs. The rules and social arrangements necessary to achieve this must take into account the characteristics of these socio-technical systems, which involve public, private, and non-profit actors, with broad impact given the scale of providers and users, and which operate globally. These characteristics reflect the type of system that is unlikely to be able to devise and monitor its own rules[61] and, hence, is unlikely to self-regulate effectively. Elinor Ostrom suggests that under these conditions there are several principles that need to be taken into account in designing rules and institutions, including support by higher authorities, establishment of clear definitions for access to the systems and clear boundaries, participation by users in devising rules, and low-cost conflict-resolution mechanisms.[62]

The government's role does not have to be "heavy-handed" or innovation stifling, but it does need to be designed to keep the online platforms, on which individuals interact in groups and with public and private organizations, accountable for their information practices. Oversight by an independent authority and auditing of organizational practices are both the types of policies that might enable individuals in groups to both actually see the information flows within and outside their groups, and also negotiate and modify in ways to better protect their privacy. If privacy is a public good and lack of privacy a public bad, then policy needs to recognize that the overall

---

59. *Id.* at 420.

60. Priscilla M. Regan, *Privacy as a Common Good in the Digital World*, 5 INFO., COMM. & SOC'Y 3, 382–405 (2002); *see* Priscilla M. Regan, *Big Data and Privacy*, *in* ANALYTICS, POLICY AND GOVERNMENT (Jennifer Bachner et al. eds., forthcoming).

61. COMM. ON THE HUMAN DIMENSIONS OF GLOB. CHANGE, NAT'L RESEARCH COUNCIL, THE DRAMA OF THE COMMONS (Elinor Ostrom et al. eds., 2002).

62. ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION (James E. Alt & Douglass C. North eds., 1990).

transmission architecture of the Internet constitutes a critical infrastructure, and that protecting privacy on the Internet is as important as protecting security and reliability. Policy may also consider whether some online platforms, such as Facebook and Google, have achieved the breadth, reach, and importance that they should be viewed as "public trustees" with government standards requiring that they operate in the "public interest."[63]

CONCLUSION

Fairfield and Engel close by stating that "[t]he highest aspiration of an academic article is not to settle a debate, but to spur further inquiry."[64] I have written this response in that same spirit and am convinced of the need for "a more balanced debate about the tensions between individuals and groups in the privacy context."[65] This debate has clearly begun and is enriched by the empirical data, theories, and insights of economists, lawyers, political scientists, psychologists, sociologists, philosophers, computer scientists, and engineers. The social dilemma of privacy has intrigued a large and growing cohort of multi-disciplinary scholars who are increasingly seeking to affect policy decisions. *Privacy as a Public Good* promises to generate more empirical and theoretical work.

63. Priscilla M. Regan & Deborah G. Johnson, *Policy Options for Reconfiguring the Mirrors*, *in* TRANSPARENCY AND SURVEILLANCE AS SOCIOTECHNICAL ACCOUNTABILITY: A HOUSE OF MIRRORS, *supra* note 57, at 162, 162–84.

64. Fairfield & Engel, *supra* note 1, at 457.

65. *Id.*