Duke Law Journal Online

VOLUME 65 FEBRUARY 2016

PRIVACY, PUBLIC GOODS, AND THE TRAGEDY OF THE TRUST COMMONS: A RESPONSE TO PROFESSORS FAIRFIELD AND ENGEL

DENNIS D. HIRSCH†

INTRODUCTION

In his classic 1967 book, *Privacy and Freedom*, Professor Alan Westin explained that humans desire neither complete isolation, nor complete exposure, as each would be a form of torture.[1] In order to live and thrive, human beings require a condition that lies somewhere between the two poles.[2] Each individual strikes this balance in his or her own way. Some wish to share more about themselves, and some less. Westin accordingly defined the right to privacy as the right to control one's personal information.[3] Modern privacy law is largely based on this foundational definition. It employs notice, choice, and purpose limitations to give individuals control over their personal information and so to realize Westin's notion of privacy.[4]

† Professor of Law, Ohio State Moritz College of Law; Faculty Director, Program on Data, Law, Ethics and Policy at Ohio State Moritz College of Law; Professor of Law, Capital University Law School. The author would like to thank Professors Shi-Ling Hsu and Brett Frischmann for their thoughtful comments, and Brian Kocak for his excellent research assistance.

1. *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 40–41 (1967).

2. *Id.* at 42.

3. *Id.* at 7 (defining privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others").

4. *See* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 242 (2013) (identifying the Fair Information Practice Principles that have formed the core of privacy law and policy for the past

In their illuminating and important article, Professors Joshua Fairfield and Christoph Engel explore a problem with this basic paradigm: when one person chooses to reveal personal information, the act frequently discloses others' personal data as well.[5] Fairfield and Engel provide a cogent and useful account of these privacy spillovers.[6] They then confront head-on the logical implication of such externalities: the law cannot provide each individual with control over his or her personal information.[7] Even if it wants to; even if it tries to; even if it perfectly implements Westin's notion of individual control, the law cannot achieve this end for the simple reason that one person's decisions to disclose his or her personal information often affect the privacy of others. "Individual control of data is a fundamentally flawed concept."[8]

Fairfield and Engel do not despair. Instead, they offer a new account of privacy regulation to supplement the traditional model grounded in Westin's ideas. Their approach is based less on notice and choice, and more on allowing groups of people to coordinate their actions and so achieve the privacy that they all desire.[9] Their theoretically and empirically well-grounded argument forces us to rethink the very project and form of privacy regulation. Fairfield and Engel do not dispute the importance of Westin's formulation of traditional, control-based privacy law. But they do create an important supplement that fills in a blind spot in contemporary privacy law and policy. This is an extremely valuable project and Professors Fairfield and Engel carry it off with rigor and elegance.

Their analysis, however, is itself incomplete. Fairfield and Engel's account of privacy, and of privacy law, focuses almost entirely on individuals who disclose information about others. It does not directly address the role that corporations play in the collection, use, and disclosure of personal information. In so doing, it skips over a

four decades); Ira S. Rubinstein, Big Data: A Pretty Good Privacy Solution 1 (2013) (unpublished manuscript), https://fpf.org/wp-content/uploads/TECH-Rubinstein-Big-Data-A-Pretty-Good-Privacy-Solution.pdf [http://perma.cc/5P5D-XGFA] (noting that Fair Information Practices (FIPs) "form the basis of all modern privacy law").

5. *See* Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 389–90 (2015); Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J.L. POL'Y FOR INFO. SOC'Y 425, 429 (2011) ("The idea is that disclosure of information by some people can reveal information about other people, to their detriment.").

6. Fairfield & Engel, *supra* note 5, at 389–90, 407–08.

7. *Id.* at 408–12.

8. *Id.* at 390.

9. *Id.* at 408–12.

significant—perhaps the most significant—part of the problem. This is intentional. Fairfield and Engel recognize that "[p]rivate companies have accumulated deep and potentially toxic pools of consumer data."[10] They make a conscious choice to focus, instead, on individuals.[11] Still, the gap is an important one. Any set of policy prescriptions that would seek to improve privacy in a meaningful way must address the business activities that contribute so significantly to the problem.[12] Fairfield and Engel's solutions do not deal with this important part of the issue.

This response seeks to fill that gap. Using some of the same economic concepts as Fairfield and Engel—specifically, public goods and the tragedy of the commons—it develops a complementary account of business use of personal information, why society should regulate it (and why the companies themselves should want this), and how to conceptualize this regulatory project. It offers not so much a criticism of Fairfield and Engel's work, as an addition to it. Their theory focuses on individuals and groups of individuals; mine, on corporations. Any solution worth its salt will need to cover both.

Part I of this response introduces more fully Fairfield and Engel's argument about privacy spillovers and their implications for privacy law and policy. Part II discusses Fairfield and Engel's call for group coordination strategies that will supplement the traditional "notice and choice" regulatory approach. This Part argues that these group-coordination strategies will likely succeed only with respect to one of the two types of privacy externalities that Fairfield and Engel identify. Specifically, it highlights the fact that such interventions do not address corporate and government uses of personal information and so fail to address the larger part of the privacy problem. Part III examines Fairfield and Engel's claim that, left unaddressed, individual privacy externalities will lead to a tragedy of the commons. Drawing on the work of Professor Shi-Ling Hsu, this Part argues that

---

10. *Id.* at 392.

11. *See id.* at 421 ("In taking this approach, we focus less on rules restraining large-scale bad actors, and more on the dilemma of groups seeking to cooperate in the face of a social dilemma.").

12. The government is also a major contributor to the privacy problem, as the National Security Agency's recent actions make clear. This article focuses on the privacy externalities that the private sector creates. Parts IV and V of this article analyze the corporate contribution. They suggest that it could produce a tragedy of the commons, and that commons-management theory provides a useful framework for addressing it. This article does not directly address governmental contributions to the privacy problem. It leaves for another day the question of how best to reduce government-created privacy injuries.

Fairfield and Engel identify a large-group externality, not a true tragedy of the commons. This distinction is an important one, as it affects the rationale for government intervention. Part IV looks further into the tragedy of the commons idea. It argues that the information economy is indeed confronting a true tragedy of the commons, although not the one that Fairfield and Engel identify. The commons is a user trust. Companies dip into and rely on this trust each time they ask a user to provide them with personal information as part of a digital interaction. They have a short-term incentive to abuse this trust for financial gain. But if they over-exploit user trust, individuals will significantly reduce the amount of personal information that they share, thereby damaging the companies themselves. In short, companies that over-exploit the trust commons will damage it and so deprive themselves of the very resource—user trust—on which they rely. This is a true tragedy of the commons. Part V looks to commons-management theory, particularly the work of Professor Carol Rose, to generate ideas as to how society might best avert this impending tragedy of the trust commons.

I. CHALLENGING THE DOMINANT PARADIGM

Professors Fairfield and Engel make two principal, highly convincing points about the nature of privacy. First, building on the work of Professor Mark MacCarthy,[13] they argue that individual decisions to disclose personal information affect the privacy of others in two ways.[14] One is immediate and direct. For example, an individual who posts on social media a photograph of herself standing with friends would thereby reveal not only her own whereabouts, but also that of others in the picture.[15] Similarly, an individual's decision to reveal her location (by carrying a smartphone, for example) can reveal the probable location of those intimates with whom she spends a lot of time.[16] Individuals also create indirect privacy spillovers. Their

13. *See* MacCarthy, *supra* note 5, at 445–68 (discussing negative privacy externalities).

14. Fairfield & Engel, *supra* note 5, at 389.

15. *Id.* at 402. The combination of location and social-media information also frequently reveals information about others. "Cell phones track individuals' location precisely, and by proxy, the locations of others. Knowledge of where one person is, augmented by knowledge of that person's social network, can help to identify and locate those who are regularly in proximity to that person." *Id.* at 402–03. In these and other such examples, an individual's decision to disclose particular pieces of information about herself can immediately and directly reveal information about others as well.

16. *Id.* at 402.

decisions to participate in the digital society—to visit a Web site, make an online purchase, carry a smartphone, use a "smart meter" for electrical consumption in their home, etc.—leave a data trail that contributes to the overall pool of personal information. Analysts can use this data to create highly accurate profiles that allow them to predict others' personal information.[17] For example, certain women made a decision to shop at Target, which revealed their purchasing habits to the store. Target then combined these customer-purchase records with public listings of live births to construct a profile of the pregnant Target shopper. It then applied this profile prospectively to its current female customers in order to predict, with great accuracy, which were pregnant.[18] The decisions of the women in the first group to disclose what they had purchased and that they had given birth allowed Target to infer latent information about the second group. This, too, is a form of privacy externality.[19]

Fairfield and Engel's second main point about the nature of privacy is that the good of living in a society that respects privacy is a nonexcludable, nonrivalrous, pure public good.[20] It is nonexcludable in the sense that if it is available to one, it is available to all. It is nonrivalrous in that one person's enjoyment of the good does not limit others' ability to enjoy it. This is an important point because markets handle negative externalities that harm public goods much less well than those that damage private goods. When an externality impacts a private good and transaction costs are low, market transactions can typically prevent the occurrence of inefficient externalities. That is one of the Coase theorem's key points.[21] For example, if A and B are neighbors, and A decides to cut down a tree on her property that will rob B of much-valued shade, this damages the "shadiness" of B's property—a private good. If B values the shadiness more than A values cutting down the tree, B can pay A to keep the tree standing.[22] In this way, a market transaction can prevent an inefficient externality.

---

17. *Id.* at 389–91.

18. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=0 [http://perma.cc/5Y42-2PXX].

19. *See id.*

20. *See* Fairfield & Engel, *supra* note 5, at 390.

21. *See* Ronald Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 42–44 (1960).

22. In a world of no transaction costs, such transactions will prevent all inefficient externalities regardless of the initial allocation of property rights. *See id.*; *see also* PETER S.

Market transactions have a much harder time accomplishing this, however, where the externality impacts a pure *public* good. The nonexcludability of public goods gives rise to collective-action and free-rider problems that greatly increase transaction costs and so can prevent deals that would have prevented inefficient externalities. Clean air is a good example. If it is provided to one, it is provided to all. It is nonexcludable. Polluters (factories, cars, etc.) emit pollutants and thus use up the clean air resource. Even if the pollution is inefficient (that is, the marginal cost of pollution control is less than the marginal cost to health and the environment of continued pollution), market transactions will not prevent it.[23] It is not in anyone's interest to organize all who must breathe the air and get them to contribute. Moreover, each individual can sit back and let the others pay for the controls. Those who do so can still breathe the air once others have improved it. Together, the collective-action and free-rider problems will prevent market transactions from addressing many inefficient externalities.

Fairfield and Engel explain that the good of living in a society that protects privacy, much like the good of living in a society with clean air, is a public good.[24] If one of us gets to live in such a society, then we all do. This means that, unlike the neighbor who pays to protect the "shadiness" of his property, few will pay to provide the good of a privacy-protective society. This confronts each of us with a "social dilemma."[25] Each gets the full benefit of sharing personal information but externalizes most of the privacy costs onto others. No one will pay us to refrain from imposing the externality because privacy in society is a public good. From an individual perspective, it therefore makes sense to continue sharing the information. But if all of us make this decision, as all of us will, this ends up creating a privacy-depleted society that few desire to live in.[26] Individual decisions prevent us from reaching a state that we, as a group, would prefer. They lead us to foul our own nest with excessive amounts of

---

MENELL & RICHARD B. STEWART, ENVIRONMENTAL LAW AND POLICY 57 (1994) (explaining that public good problems would "solve themselves . . . if it were costless to bargain").

23. *See* JAMES SALZMAN & BARTON H. THOMPSON, JR., ENVIRONMENTAL LAW AND POLICY 22–23 (4th ed. 2014) (describing the collective-action and free-rider problems in an environmental context); *see also* MENELL & STEWART, *supra* note 22, at 54–55 (applying these concepts in the air pollution context).

24. Fairfield & Engel, *supra* note 5, at 423–33.

25. *Id.* at 387, 422, 456.

26. *Id.* at 423.

personal information, much as individual decisions to operate a factory, drive a car, or run a lawn mower produce the smog that makes the air unhealthy for all.

In Fairfield and Engel's capable hands, this insight is a powerful one, indeed. They use it to explain the so-called "privacy paradox," in which people say in surveys that they do not want to reveal their personal information to others, yet in practice they do so all the time. Most have chalked this up to a failure in notice and choice. Fairfield and Engel show, however, that it is the social dilemma that causes it: "In weighing important decisions about privacy, individual and group incentives diverge. . . . [I]ndividuals' fully informed privacy decisions tend to reduce overall privacy, even if everyone cherishes privacy equally and intensely."[27] This insight into a problem that has bothered privacy theorists for years is itself worth the price of admission.

Fairfield and Engel further use their externality and public-goods analysis to identify an important gap in privacy law and policy, and offer a way to fill it. As stated above, they explain that notice, choice, and purpose limitation are insufficient in a world of privacy externalities.[28] In a highly original argument they maintain that, in order to prevent such externalities, law and policy must provide *groups* with the means to overcome the social dilemma that leads to an undesired, privacy-depleted society.[29] "[G]roups must be given tools to create the public good of privacy and resist the public bad of readily available intrusive information . . . . The relevant legal tools, therefore, should be redesigned to focus less on individual knowledge and empowerment and more on facilitating groups' collective protection of their privacy."[30] Fairfield and Engel draw on the neoclassical and behavioral economics literature, particularly the experimental evidence on group coordination, to suggest subtle interventions that would allow groups more easily to coordinate and so to achieve their members' true preferences.[31] These intelligent, theoretically- and empirically-grounded suggestions include reminding users of social networks that they are repeat players in order to induce them to cooperate;[32] showing users that they benefit

27. *Id.* at 423; *see id.* at 400.
28. *Id.* at 389.
29. *See id.* at 388–89.
30. *Id.* at 395–96.
31. *Id.* at 396, 433–56.
32. *Id.* at 438–39.

from others' privacy-protective actions, and so leveraging their "inequity aversion" to encourage them to act more responsibly;[33] providing people with evidence that others are protecting their privacy, and so tapping into their human desire to reciprocate by doing the same;[34] increasing the payoff that individuals receive from privacy-friendly behavior;[35] and other interesting and useful techniques.[36] These suggestions add valuable arrows to the quiver of privacy law and policy.

II. WILL GROUP-COORDINATION SOLUTIONS REALLY SOLVE THE PROBLEM?

Group-coordination solutions are not sufficient, however. Fairfield and Engel focus on the spillovers that *individuals* create. For the most part, they do not address the privacy harms that businesses produce even though these, too, constitute negative externalities.[37] As was mentioned above, they do this intentionally. Fairfield and Engel certainly recognize that "[p]rivate companies have accumulated deep and potentially toxic pools of consumer data."[38] They choose to focus more on groups of individuals trapped in a social dilemma, and less on large-scale business contributors.[39] Still, it is worth pointing out

---

33. *Id.* at 439, 445–46.

34. *Id.* at 447–48.

35. *Id.* at 441, 443, 449–50.

36. Fairfield and Engel summarize them as follows:

> This Article mines the behavioral-economics literature to find new approaches to privacy protection that permit groups to sustain cooperation and protect privacy even without direct government intervention. We suggest a focus on empowering groups. We suggest leveraging inequity aversion, reciprocity, and normativity to lessen exploitation among group members. We suggest positive framing to promote altruism. We suggest that communication and (private) sanctions are key components of group coordination. With these tools, groups may be able to sustain privacy without governmental intervention and the challenges and distortions that flow therefrom.

Id. at 396 (footnotes omitted).

37. Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn From Environmental Law*, 41 GA. L. REV. 1, 28–30 (2006).

38. Fairfield & Engel, *supra* note 5, at 392.

39. *See id.* at 421 ("In taking this approach, we focus less on rules restraining large-scale bad actors, and more on the dilemma of groups seeking to cooperate in the face of a social dilemma.").

Fairfield and Engel argue that Congressional gridlock will prevent legislative solutions to corporate-privacy violations, and that interventions focused on individuals will be easier to achieve. *See id.* at 419–20. The environmental experience has been the opposite. Laws that seek to regulate individuals have proven highly controversial. Congress has found it easier politically to regulate corporate contributors and most environmental laws take this approach. It may be

that their solutions address the smaller part of the problem. If privacy law is to achieve its aims, it must address the business dimension.[40] Fairfield and Engel invoke the environmental analogy,[41] and it is apt here. Businesses and individuals both contribute to environmental degradation. But the business contribution is larger and so environmental law focuses on it. The same is true in privacy. Although individuals do impose privacy externalities on one another, companies contribute greatly to the problem. Any set of policy prescriptions that would seek meaningfully to improve the privacy picture must address the corporate contributions.[42]

Even with respect to the privacy externalities that individuals create, Fairfield and Engel's group-coordination solutions are likely to work better for the first type of privacy externality—the direct spillovers—than for the second, the data trails that fuel data analytics. Most individuals can intuitively grasp that posting a group photo affects the privacy of others. They may even be able to see that disclosure of their location data can provide clues as to the whereabouts of their intimates. Group-coordination policies that work by making individuals more aware that they are repeat players, or that privacy-friendly behaviors can produce pay-offs, have a chance of working in such situations.

It is much harder to see how such group-coordination strategies could address the second category of spillovers. As Fairfield and Engel themselves recognize, most individuals understand neither the data stores they are helping to create nor the ways in which data analysts can use such information to produce actionable insights.[43] No one, not even the analysts themselves, can foresee the insights that analytics will reveal from a particular data set.[44] Given these deep informational deficits, how can group-coordination strategies premised on repeat play, individual payoffs, inequity aversion, or

---

that less intrusive, group-coordination methods will prove less controversial than government regulation of individuals. But this is due to the regulatory strategy (group-coordination vs. direct regulation) and not to the regulatory target (individuals vs. corporations).

40. The government is also a major contributor to the privacy problem, as the National Security Agency's recent actions make clear.

41. Fairfield & Engel, *supra* note 5, at 419.

42. Parts IV and V of this article analyze the corporate contribution.

43. Fairfield & Engel, *supra* note 5, at 390.

44. VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 173 (2013) (explaining that "unimagined" secondary uses emerge from personal data, and that this makes it harder to protect individual privacy with respect to those data).

reciprocity have their intended effect? Such strategies depend on individuals having a basic understanding of the data they are releasing and how it impacts privacy. With respect to big data and data analytics, that understanding is largely missing. When it comes to predictive analytics, then, individuals will likely have a much harder time employing group-coordination strategies to protect themselves. Instead, it may become necessary for the public to confront difficult questions about which predictions companies and governments should be able to act upon, and which they should not. Should it be permissible for a company to predict someone's risk of suffering from a serious mental or physical illness in the future, and then use this as the basis for denying that person employment, housing, or a loan? Data analytics can make such predictions with accuracy.[45] What are appropriate, and what are inappropriate, uses of this power?

These are not questions of group coordination. They are deep questions of values that require us to think about the type of society we want to have and government's role in achieving it. Data analytics can produce both highly beneficial social and economic outcomes, and harmful privacy and discriminatory impacts.[46] Society needs a mechanism for identifying, and preventing, those data-analytics applications for which the harms manifestly outweigh the benefits. Elsewhere, I have argued that the Federal Trade Commission (FTC) could use its unfairness authority to make such determinations.[47] Section 5 of the Federal Trade Commission Act authorizes the FTC to declare "unfair" and unlawful those business activities that substantially injure consumers, that consumers cannot protect themselves against, and that create more harms than benefits.[48] This should allow the FTC to examine specific data-analytics applications that substantially injure consumers (by, for example, denying them credit or a job), weigh the benefits that they produce against the harms that they create, and determine, on balance, whether the particular application is "unfair." In this way, the FTC could employ

45. *See* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 18 (2014) (explaining that predictions increasingly determine "people's life opportunities—to borrow money, work, travel, obtain housing, get into college, and far more").

46. Dennis D. Hirsch, *That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority*, 103 KY. L.J. 345, 346 (2014) (describing a number of these benefits and harms).

47. *Id.* at 347, 353–57.

48. 15 U.S.C. § 45 (2012).

its unfairness authority to sort data-analytics applications that are appropriate and fair, from those that are inappropriate and unfair, and prevent the latter. This would bolster public support for those data-analytics applications in which the benefits outweigh the harms. The FTC's unfairness authority may, or may not, turn out to be the best vehicle for making these calls. But society will need to find some way of making them if it is to protect itself against data analytics' most harmful impacts and so unlock its tremendous benefits. Fairfield and Engel's group-coordination strategies are unlikely to achieve this.

III. TRAGEDIES TRUE, AND LESS TRUE

Economic theory can provide insight not just into individual privacy externalities, but into corporate ones as well. To see this, it is necessary to modify Fairfield and Engel's discussion of the tragedy of the commons.

Fairfield and Engel explain that, just as environmental externalities can pollute nonexcludable resources such as clean air or clean water, the privacy externalities that individuals impose on one another could lead to a tragedy of the commons with respect to the public good of privacy.[49] "[T]he struggle for privacy is destined to become a tragedy."[50] This claim employs a common, though not the most precise, usage of the term "tragedy of the commons." As Professor Shi-Ling Hsu has explained, scholars have used the term to refer to two distinct phenomena, only one of which is a true tragedy of the commons.[51] First, scholars use the term to refer to "large-group externality problems in which resource users impose externalities upon a larger population, without necessarily harming themselves" and without reducing others' ability to exploit the resource.[52] For example, those who pollute the air externalize most of the costs onto the large group composed of individuals who breathe the air. They bear only the small fraction of the cost associated with their

49. Fairfield & Engel, *supra* note 5, at 391.

50. *Id*. They later explain that privacy externalities are more likely to cause a "drama" of the commons than a "tragedy" because, as Elinor Ostrom and others have pointed out, some communities have found ways to overcome the social dilemma that otherwise would lead to tragedy. *Id.* at 395. This does not alter their claim that the current incentive structure will lead to dynamic that Garrett Hardin termed a "tragedy of the commons" with respect to privacy. It just refers to the fact that communities need to struggle in order to overcome this dynamic.

51. Shi-Ling Hsu, *What IS a Tragedy of the Commons? Overfishing and the Campaign Spending Problem*, 69 ALBANY L. REV. 75, 78 (2005).

52. *Id.* at 81.

membership in this larger group. Moreover, in the absence of a regulatory or some other property-rights regime, the factory's emissions do not reduce other polluters' ability to emit.[53] Given that each polluter gains the full benefit of its emissions but bears only a small fraction of the cost (the same fraction as that borne by each other member of the breathing public), individual factory owners or other emitters will continue to emit regardless of the costs and the air will become polluted.

Hsu distinguishes these situations from true tragedies of the commons in which resource users exploit a nonexcludable resource in such a way that they "detract from their *own* ability to continue to exploit the resource."[54] Fisheries provide a clear example of this second usage.[55] A fishery naturally replenishes itself as the fish reproduce. If the fishers harvest the resource in a sustainable way, the fishers will have fish to catch well into the future. However, if they take too many fish at once, this can cause the fish population to crash and thus destroy the fishing ground. When this happens, the fishers themselves lose, not just in their capacity as members of the broader public, but in their role as resource users who no longer have a resource to exploit.

Resources like a fishery are partially rivalrous.[56] They are nonrivalrous up to a point. So long as the fishers do not harvest too many fish, their exploitation of the resource does not constrain others' ability to use it. But once the exploiters cross a threshold—once they remove too many fish in too short a time—the resource crashes. At that point, the resource becomes rivalrous in consumption.[57] Other partially rivalrous resources would include aquifers that lose their ability to recharge themselves when

53. *Id.* at 94. The clean-air resource is therefore both nonexcludable in the sense that all can make use of it, and nonrivalrous in the sense that one user's exploitation of the resource (emission of air pollutants) does not reduce another's ability to emit as well. This makes it a pure public good in that it is both nonexcludable and nonrivalrous. *See* Brett M. Frischmann, *An Economic Theory of Infrastructure and Commons Management*, 89 MINN. L. REV. 917, 943 (2005).

54. Hsu, *supra* note 51, at 78. Professor Jane Yakowitz makes an interesting case for treating de-identified personal information used for research purposes as a partially rivalrous, nonexcludable resource. *See generally* Jane Yakowitz, *The Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1 (2011).

55. *Id.* at 100–05.

56. Frischmann, *supra* note 53, at 951–53. Frischmann refers to such goods as "partially (non)rivalrous," rather than as "partially rivalrous." *Id.* at 952. The meaning is the same.

57. *Id.* at 953.

communities withdraw too much water too quickly,[58] roadways that clog up from traffic congestion,[59] or Garrett Hardin's example of the common grazing field that cannot regenerate its grass due to overgrazing.[60]

Resources of this type share three key features. The first is the "stock" variable—the core resource that is potentially renewable.[61] A fishery, aquifer, common grazing field, or roadway each represents a type of stock. The second is the "flow" variable—the rate at which the good the resource produces is extracted.[62] Fish, fresh water, grass, and open roadways for transit would each constitute a flow. The third is the "fringe" value—the number of resource units (fish, fresh water, grass, open road) that can be harvested without impairing the resource's ability to regenerate.[63] If appropriators harvest more than the fringe, they end up destroying the stock and reducing (or eviscerating) the flow. If, on the other hand, they harvest the source in a sustainable manner, then the stock can continue to generate the fringe indefinitely.[64]

In his classic essay, *The Tragedy of the Commons*, Garrett Hardin uses the term interchangeably to refer both to large-scale externality problems (for example, air pollution) and to true tragedies of the commons. However, he focuses on true tragedies involving partially rivalrous resources, and not on large-group-externality problems involving nonrivalrous resources.[65] Hardin's article centers on the cattle herders who graze their animals on a common grazing field.[66] The grass will renew itself so long as the cattle herders do not over-graze it. However, if they add too many cattle to the field, the animals will eat the grass down to its nubs so that it no longer regenerates.[67] This makes the common grazing field a partially rivalrous resource. It provides a sustainable yield of grass up to a

58. Hsu, *supra* note 51, at 88.

59. *Id.* at 95.

60. Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243, 1244 (1968).

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

62. *Id.*

63. *Id.*

64. *Id.*

65. *See generally* Hardin, *supra* note 60 (focusing on the effects of overpopulation on resources such as food and energy itself).

66. *Id.* at 1244.

67. *Id.*

point. But if the resource use exceeds that threshold—if the harvest exceeds the fringe—the grass resource, much like a fishery, will collapse.

Hardin's key point is that rational herder will not stop at this threshold.[68] Since the field is open to all herders, an individual herder captures the full benefit of each animal that he adds to the field but shares the cost, in terms of the grass consumed, with all the other herders. Acting rationally, the herder will add another animal to the field, and then another, and another. So will the other herders.[69] This leads to the destruction of the field. Having harvested more than the fringe value, the herders destroy the stock and decimate the flow. As a result, they end up destroying the very resource—the grass—on which they themselves depend. They hurt themselves, not just as members of the general public, but in their capacity as cattle herders. They ruin their own livelihood. That is why the result is *tragic*, and not just sub-optimal or harmful. "Ruin is the destination to which all men rush, each pursuing his own best interest in a world that believes in freedom of the commons."[70]

Hsu's distinction between "true traged[ies] of the commons," such as Hardin's cattle herder example, and "large-scale externality problems," such as air pollution,[71] is important when it comes to the rationale for government intervention. With respect to large-scale externalities it will make economic sense for emitters to install pollution controls so long as the marginal cost of control is less than marginal cost of the externality imposed on the public.[72] This could justify a public policy requiring such controls. But a polluter, acting rationally, will resist such government intervention.[73] Each polluter bears only a small fraction of the cost of the pollution—the same as that borne by any other member of the public who breathes the air—but would have to bear the full costs of installing the pollution controls. The polluter's interest will lie in less control, not more.

Not so for a true tragedy of the commons. Here, in the absence of government intervention or some other means of social control, the resource users will end up destroying the resource on which they

68. *Id.*
69. *Id.*
70. *Id.*
71. Hsu, *supra* note 51, at 92.
72. *Id.* at 93.
73. *See id.* at 92.

themselves rely. This provides an "additional, simple and compelling justification [for government intervention]: save the resource users from themselves."[74] An enlightened cattle herder, able to think long-term and foresee the inevitable tragedy, should favor such an intervention so long as it constrains all cattle herders and does, in fact, avert the tragedy.

Fairfield and Engel's privacy spillovers create a large-scale externality problem, not a true tragedy of the commons. As they describe it, an individual's release of information about self and others contributes to the overall lack of privacy in the culture.[75] The individual suffers the cost of living in such a culture. This injury is the same as that which any other member of the public suffers.[76] Moreover, the individual's release of information constrains neither her own, nor anyone else's ability to disclose information and use up the privacy resource in the future. In this respect, an individual's privacy spillovers are analogous to air pollution. Releases of information, like emissions of air pollutant, impose a cost on the broader public that the emitter bears only insofar as she is a member of that larger group. There is no threshold beyond which the privacy resource, or the clean air resource, collapses and prevents future appropriation. Privacy, for Fairfield and Engel, is a nonexcludable, nonrivalrous public good, much like clean air.[77] Individual release of information creates a large-group externality, not a true tragedy of the commons.

This matters for two reasons. First, as explained above, large-group externalities create a weaker rationale for social control than do true tragedies of the commons. That may be why Fairfield and

74. *Id.* at 94.

75. Fairfield & Engel, *supra* note 5, at 423.

76. Where A releases B's personal information (for example posts a group photo in which B appears), then A's action affects B more than it does a member of the general public. B's privacy is a private good, not a public one. However, where A, B, C, D, E, etc. are all posting many photos and causing many other privacy spill overs, this affects the state of privacy in society. That is the focus of Fairfield and Engel's analysis. They look at all of the individual acts combined and the broader effect that they have on privacy in society. Living in a society that provides privacy is a public good. *See, e.g.*, *id.* at 388–92.

77. *Id.* at 387, 423 (defining "public good" as a "nonrival and nonexcludable resource" and arguing that "privacy is a public good as that term is strictly defined in the economics literature"). Fairfield and Engel examine the possibility of conceptualizing privacy as an impure public good, *id.* at 442–44, but conclude that the pure public good characterization makes more sense "if one considers the broad run of the Internet . . . ." *Id.* at 444.

Engel focus on group-empowerment solutions that entail a "reduced need for government intervention."[78]

Second, while it almost always makes sense for the public to take action in order to prevent a true tragedy of the commons, the same is not necessarily true for large-scale externalities. Take air pollution. From an economic perspective, it makes sense to control air emissions only so long as the marginal cost of controls is less than the marginal social benefit in terms of pollution reduced.[79] The same would hold true for the individual privacy spillovers on which Fairfield and Engel focus. Society may wish to reduce them if this can be achieved in a cost-effective way. But if the marginal cost of control is greater than the marginal benefit, then controls—even those produced by non-interventionist group-coordination solutions—would not make economic sense. Fairfield and Engel assert that society should seek to reduce individuals' privacy spillovers. However, they do not show that the marginal benefit of doing so will necessarily be greater than the marginal cost. In this regard, they do not demonstrate that the activity is socially harmful or that intervention is necessarily warranted.[80]

IV. THE TRAGEDY OF THE TRUST RESOURCE

The over-use of personal information is leading to a tragedy of the commons but it is not the one that Fairfield and Engel identify. Instead, it is a tragedy of the trust commons. All economies depend on trust.[81] "We trust that merchants will accept the small, green pieces of paper that we've earned in exchange for goods and services. We trust that airplanes will arrive safely and to the correct airport. We trust that professionals in our service will act in our best interest . . . ."[82] The information economy is no different. When we engage in a digital transaction, visit a Web site, enter a search query,

78. They offer an approach that entails a "reduced need for government intervention," *id.* at 398, and that "sustain[s] cooperation with minimal outside intervention." *Id.* at 420.

79. Distributional and ethical concerns may alter this analysis in particular cases.

80. This is not an idle question. Fairfield and Engel's group-coordination solutions could impose significant marginal costs. For example, interventions that reduce the amount of information available for data analytics could prevent analysts from making health- or safety-promoting predictions.

81. *See generally* Neil M. Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, STAN. TECH. L. REV. (forthcoming 2016), http://ssrn.com/abstract=2655719 [http://perma.cc/PS4D-UN78] (analyzing the role of trust as a positive function of privacy).

82. *Id.* (manuscript at 3–4).

or make a purchase from an online store, we trust the provider to supply us with goods and services that will not hurt us, just as we do in the brick-and-mortar economy.[83]

In order to participate in the digital economy, we must also trust in another way. The information economy is premised on the sharing of personal information; it is "mediated by information relationships" to a far greater extent than prior economies.[84] Participating in the information economy accordingly requires us to trust others with our personal information. This particular kind of trust—"digital trust"—consists of our faith that the providers of digital goods and services will use our personal information to benefit—not hurt—us.

The information economy depends on digital trust.[85] If people were to become convinced that the search engines, social media sites, web sites, and other such providers were using their personal information to hurt them, they would share less of it.[86] For example, in the wake of the massive Target data breach in which hackers gained access to an estimated forty million credit card numbers and seventy million addresses, phone numbers and other pieces of personal information,[87] approximately one in three shoppers interviewed said that they planned to use cash more frequently.[88] They temporarily lost trust in digital credit card transactions and started to move away from them.

The same thing could happen on a broader scale. If users became convinced that sharing their personal information with digital providers would hurt them, they would start to withhold this data. For example, researchers from MIT and Digital Fourth found that, in the wake of the Snowden revelations, Google searches for controversial

83. *See id.* (manuscript at 4).

84. *Id.*

85. *See id.* (manuscript at 45).

86. *Id.* (manuscript at 6) ("Without trust, people share less information, bad information, or no information at all. They become anxious, bewildered, and suspicious. They lie or self-censor otherwise beneficial information.").

87. Matt Townsend, Lauren Coleman-Lochner & Lindsey Rupp, *Target Is Expected to Pursue Its First Outside CEO*, BLOOMBERG BUS. (May 6, 2014, 4:27 PM), http://www.bloomberg.com/news/articles/2014-05-06/target-is-expected-to-pursue-its-first-outside-ceo [http://perma.cc/SX8G-WYYS].

88. Paula Rosenblum, *In Wake of Target Data Breach, Cash Becoming King Again*, FORBES (Mar. 17, 2014, 5:11 PM), http://www.forbes.com/sites/paularosenblum/2014/03/17/in-wake-of-target-data-breach-cash-becoming-king-again [http://perma.cc/AM9F-3XZJ].

terms decreased.[89] This affected not just searches related to terrorism or bomb-making, but also searches for terms such as "herpes," "eating disorder" and "erectile dysfunction."[90] A 2016 Pew Research Center study, consisting of both a survey and focus groups, concluded that Americans' willingness to share personal information with commercial entities was "contingent" on whether the benefits of doing so outweighed the privacy and security risks.[91] Study participants expressed concern about the safety and security of their information and anger about the ways in which companies use it.[92] The study showed that their willingness to share such information "depends on the circumstances of the offer, *their trust in those collecting and storing the data*," and their sense of how the company will share or use the data after collecting it.[93] Overall user trust in the digital economy is not only a vital resource; it is also an open-access, partially rivalrous one. No one can fence it off. Particular companies may enhance, or deplete, overall user trust in society. They may try to protect user trust in their particular goods or services. But, in the absence of laws or other forms of social control, they cannot prevent others from dipping into the well of overall user trust, or from diminishing it through abusive behaviors.

Trust naturally replenishes itself. It is a renewable resource. After a time, most Target customers likely went back to using credit cards, and most Google users likely returned to submitting controversial searches. However, if trust absorbs too many body blows, it can crash. The Great Recession of 2008 provides a recent example of this in an analogous area. A succession of shocks led investors, companies, and banks to lose faith in borrowers and in financial markets. They stopped lending and the economy ground to a halt. The Great Recession consisted not just of a collapse in stock prices; it also involved a collapse of trust. The events of 2008 show that the trust resource can reach a point of collapse and that, when it does, the economic consequences can be severe. The same could

89. Alex Marthews & Catherine Tucker, Government Surveillance and Internet Search Behavior 4 (Apr. 29, 2015) (unpublished manuscript), https://mitsloan.mit.edu/shared/ods/documents/Tucker_WP_2015_Government.pdf&PubID=14380 [https://perma.cc/BRX8-L9FK].

90. *Id.* at 35.

91. LEE RAINIE & MAEVE DUGGAN, PEW RESEARCH CTR., PRIVACY AND INFORMATION SHARING 2 (2016), http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf [http://perma.cc/6GL9-7XGQ].

92. *Id.*

93. *Id.* at 3.

happen with the digital trust on which the information economy depends.[94]

Digital trust, then, is a type of stock for the information economy. Society naturally generates it.[95] Each trustworthy digital interaction reaffirms and enhances it, and each abuse of our personal information erodes it. The trust resource can bear quite a few of these abusive acts. As shoppers' use of their credit cards demonstrates, digital providers can consume the "fringe" amount of trust without causing a collapse. But if the abuse of trust passes a certain threshold, if digital entities consume more than the "fringe," people will start to withhold it in a substantial way. They will refrain from participating in the information economy, turn to cash, and submit only innocuous search requests. The flow of trust, and the personal information that it carries with it, will diminish. Like a fishery, the digital trust resource will collapse for a time until careful tending can bring it back.

The open-access, partially rivalrous digital trust resource is subject to the tragedy of the commons. Each company that invests insufficiently in data security and experiences a breach, takes advantage of user ignorance to scoop up sensitive personal information,[96] sells user data to criminals,[97] or otherwise abuses user trust for financial gain captures the full benefit of doing so, but shares at least some of the cost, in terms of the digital trust eroded, with all other digital providers that depend on that trust to support the flow of personal information. As a result, each appropriator of the digital trust resource will continue to take greater and greater advantage of users' personal information, notwithstanding the fact that doing so erodes the resource as a whole.

This is what we see. Much like fishers in an open-access fishing ground, information-economy companies scoop up more and more of

---

94. People may react more strongly to a breach of financial trust where their financial assets are at stake than they would to a breach of digital trust where their privacy is at issue. However, the difference may be more of degree than of kind. Loss of privacy can lead to financial harm where, for example, it results in identity theft.

95. Indeed, as a species whose great success is in some respects premised on its ability to cooperate, trust, including digital trust, may be in our DNA in addition to being in our culture.

96. *See infra* note 98 and accompanying text (describing cell phone flashlight apps that surreptitiously capture user's personal information contained on the phone).

97. One of the major U.S. data brokers, Experian, reportedly sold individuals' personal information to an underground identify theft service called Superget.info that had posed as a legitimate private investigator. *See Experian Sold Consumer Data to ID Theft Service*, KREBS ON SECURITY (Oct. 20, 2013), http://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service/ [http://perma.cc/K2TD-XSC9].

our personal information for the gain that they might achieve from it. Cell phone flashlight apps that quietly capture the user's location, contact list, and even photographs, even though this personal information has nothing to do with the flashlight service that the app provides, provide a particularly salient example.[98] There are many such abuses of user trust. This dynamic could lead to overuse of the common resource, digital trust, on which many businesses rely. Digital providers could consume more than the digital trust fringe and cause damage to the trust resource. In the same way that banks and financial houses started withholding credit during the Great Recession, so too would individuals start withholding their personal information. This would be a true tragedy of the commons. Like the cattle herders' common grazing field, or the fishing boats' fishing ground, the providers of digital goods and services would have destroyed the very resource—user trust—on which they themselves depend. What was individually rational would turn out to be collectively ruinous.

Is this already taking place? No. There are few indications that a collapse in digital trust is imminent. Could it happen? Further research will be required to assess this in a rigorous way. Initial evidence, such as the move to cash after the Target data breach, the change in post-Snowden Google searches, and the recent Pew Research Center study[99] suggest that it could. Indeed Fairfield and Engel, writing about the NSA's access to commercial information, describe how "[c]itizens have begun to censor themselves online. Surveillance has already chilled discourse. Socially, large pools of corporate-gathered data damage the societies that generate them."[100] A collapse of the digital trust resource may await us.

Framing the issue in this way has important implications. As Professor Shi-Ling Hsu has explained, it strengthens the case for public intervention.[101] Not only are individuals facing a social dilemma that results in a large-group externality problem, but information-economy businesses are confronting a social dilemma of their own that could produce a collapse of the digital trust resource on which

98. *See* Robert McMillan, *The Hidden Privacy Threat of . . . Flashlight Apps?*, WIRED (Oct. 20, 2014, 6:30 AM), http://www.wired.com/2014/10/iphone-apps [http://perma.cc/63VP-AQH9] (discussing cell phone apps that surreptitiously capture such information).

99. *See supra* notes 89–93 and accompanying text.

100. Fairfield & Engel, *supra* note 5, at 433.

101. *See* Hsu, *supra* note 51, at 93–94.

they depend. The case for intervention is stronger when the goal is to save the industry from hurting itself.

Reframing the issue as one of trust, rather than one of privacy, also reframes the policy debate in a useful way. As Professors Richards and Hartzog have explained, the policy discourse today typically views privacy protection as a cost and so pits it against economic growth.[102] Framing the issue in terms of the preservation of trust, rather than the protection of privacy, shows that individuals' interests and those of information-economy businesses are, in fact, aligned.[103] Individuals want to be able to share their personal information without being hurt. They want to be able to trust digital providers. Businesses want to preserve the digital trust resource that is so important to their long-term success. They should support policies that rein in abuses, limit trust consumption to the fringe, and ensure the sustainability of the digital trust resource and of the information economy as whole.

V. STRATEGIES FOR MANAGING THE TRUST COMMONS

How should society go about preventing the destruction of the digital trust resource? What kind of intervention is appropriate? What is likely to prove most effective? Notice, choice, and purpose limitation—the three pillars of traditional privacy regulation—are insufficient.[104] The proliferation of digital sensors and intermediaries makes it increasingly difficult to provide effective notice of collection. The growth of data analytics, in which secondary uses are frequently not known in advance, makes it harder to provide advance notice of use.[105] Without effective notice of collection and use, there can be no meaningful consent.[106] Data analytics, which is premised on finding new secondary uses of personal information, may be incompatible

102. *See* Richards & Hartzog, *supra* note 81 (manuscript at 5) ("Privacy is a tax on profits, a drain on innovation, a dangerous and naïve assumption, and a burden on the individual to fend for herself in the digital thicket.").

103. *Id.*

104. *Id.* (manuscript at 41).

105. Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?* 5 (N.Y. Univ. Pub. Law and Legal Theory, Working Paper No. 357, 2012), http://lsr.nellco.org/cgi/viewcontent.cgi?article=1359&context=nyu_plltwp [http://perma.cc/2PWS-QDLT] (explaining that big data causes problems for notice and consent).

106. *Id.*

with purpose limitation.[107] For each of these reasons, traditional privacy regulation will not prevent the tragedy of the trust commons.

Neither will Fairfield and Engel's group-coordination strategies. Companies, not individuals, confront the social dilemma that threatens the trust commons. Thus, while group-coordination solutions that focus on individuals may improve the situation to some degree, they will not avert the tragedy of the trust commons.[108]

There is a body of theory that may prove instructive. In the environmental arena, scholars and policymakers have devoted quite a bit of thought to how best to preserve the commons. If the trust-preservation issue is, at bottom, a commons problem, then this body of work could prove quite relevant. This brief essay cannot fully survey this very interesting and useful literature, but it can initiate the discussion.

Professor Carol Rose's work is particularly instructive. In her classic article, *Rethinking Environmental Controls: Management Strategies for Common Resources*, Rose identifies the four principal strategies of commons management:[109] (1) *Do-Nothing*, in which there is no intervention and the resource remains "an open access commons"; (2) *Keepout*, under which existing resource users can continue to exploit the commons, but newcomers are barred from doing so; (3) *Rightway*, in which there is regulation of "the way in which the resource is used or taken, effectively prescribing the methods by which users may take the resource"; and (4) *Property*, which allocates property rights in the resource and distributes these rights among the resource users.[110]

---

107. *See generally* Tene & Polonetsky, *supra* note 4 ("[This article] seeks to reconcile the current technological and business realities with the data minimization and purpose limitation principles . . . [which are] antithetical to big data . . . .").

108. Fairfield and Engel's group coordination strategies might work for groups of companies. For example, policy interventions that increased business awareness of the possible collapse in digital trust might trigger more privacy-friendly behavior. Self-regulatory industry initiatives with respect to privacy suggest that group coordination of this type is possible, even if difficult to achieve. This might be another potential application of Fairfield and Engel's fertile ideas.

109. *See* Carol Rose, *Rethinking Environmental Controls: Management Strategies for Common Resources*, 1991 DUKE L.J. 1, 9–10.

110. *Id.* In constructing this list, Rose builds on the work of economist Stephen Cheung. *See* Stephen Cheung, *The Structure of Contract and the Theory of a Non-Exclusive Resource*, 13 J.L. & ECON. 49, 64 (1970). Assuming that the resource were a fishery, *Do-Nothing* would leave it unprotected, allowing anyone and everyone to harvest as many fish as they desired. *Keepout* would allow established fishers to continue to use the fishery but bar newcomers. *Rightway*, would regulate the technologies that fishers could use by, for example, allowing pole fishing but

Rose explains that the cost of a management strategy is actually the sum of three distinct types of costs: (1) *Administrative or System Costs*, which are "the system-wide costs of running a management strategy, including organizational and policing costs"; (2) *User Costs*, which refer to resource exploiters' expenditures on the technologies or other controls required to reduce their impact; and (3) *Overuse or Failure Costs*, which encompass "damage caused by resource depletion" leading up to and including collapse of the resource.[111] Rose contends that society should examine how each of the four principal-management strategies applies to the resource in question and then "choose the least-cost management strategy, that is, the one with the lowest mix of [costs]."[112]

Finally, Rose argues that the outcome of this analysis is likely to depend on pressure that users are putting on the resource.[113] When the resource exploitation is minimal, and the pressure is low, *Do-Nothing* is likely to provide the lowest mix of system, user, and failure costs.[114] As the pressure on the resource begins to grow, the *Keepout* strategy begins to look more attractive.[115] It incurs some organizational and policing costs but it reduces failure costs. As the pressure continues to intensify, *Keepout* incurs greater policing costs.[116] *Rightway* may then provide the best solution. The *Rightway* approach is to "permit the outsiders to enter, but to control the means by which [exploiters] can take the resource."[117] Finally, as the resource exploitation nears maximum intensity, even *Rightway* may not sufficiently manage failure costs. In such situations, a *Property* regime, "in which we figure out how large a total [take] is acceptable and auction off the rights as individualized entitlements," may offer the lowest mix of costs.[118]

---

not allowing trawling. The fourth strategy, *Property*, would set a cap on the overall allowable take of fish and then auction harvest rights to the highest bidder. Rose, *supra* note 109, at 9–10.

111. Rose, *supra* note 109, at 12.

112. *Id.* at 14.

113. *Id.* at 12–13.

114. *See id.* at 17 (stating that, under a *Do-Nothing* strategy, "[t]here are no administrative costs for organization and policing; no user technology is specifically dedicated to control; and because no one is trying very hard to get the resource, overuse or depletion costs are still low, if they are felt at all").

115. *Id.* at 18–19.

116. *Id.* at 19.

117. *Id.*

118. *Id.* at 21.

Without additional research it is hard to identify accurately the degree of pressure on the digital trust resource. The evidence to date suggests that it is greater than zero. As early as 2000, a study found that if consumers felt more comfortable about online privacy they would spend up to $6 billion more annually on the Internet.[119] In a 2000 survey, 68 percent of respondents reported that they were "not at all comfortable" having their online browsing and shopping habits linked to their personal identities.[120] As was mentioned above, in a 2014 poll taken soon after the Target data breach, 32 percent of shoppers said that they intended to make more purchases with cash rather than cards.[121] TRUSTe's annual Privacy Index shows that the percentage of Internet users who trust businesses with their information online has fallen from 59 percent in 2012, to 57 percent in 2013, to 55 percent in 2015.[122] The 2016 Pew Research Center study, discussed above, found that Americans weighed the provider's trustworthiness in deciding whether to share their personal information with it.[123] This initial research suggests that there is at least some pressure on the digital trust resource. The days of treating it as inexhaustible—of the *Do-Nothing* approach—are over.

It seems equally clear that we are not yet at maximum pressure. The digital economy is functioning reasonably well and does not seem to be on the verge of collapse. This suggests that a *Property* regime is not yet required. Even if the pressure were intense, *Property* may not be the lowest-cost option in this situation. The system costs of defining and enforcing property rights in "digital trust" would be much higher than those required to define and police property rights in fish or even in air emissions.[124] Although the time for *Do-Nothing* has passed, the time for *Property* has not yet arrived.

---

119. Jonathan W. Palmer, Joseph B. Bailey & Samer Faraj, *The Role of Intermediaries in the Development of Trust on the WWW: The Use and Prominence of Third-Parties and Privacy Statements*, 5 J. COMP.-MEDIATED COMM., no. 3, Mar. 2000, at 1, 5 http://jcmc.indiana.edu/vol5/issue3/palmer.html [http://perma.cc/GD3J-2HFM].

120. *Business Week/Harris Poll: A Growing Threat*, BLOOMBERG BUS. WEEK (Mar. 20, 2000), http://www.businessweek.com/2000/00_12/b3673010.htm [http://perma.cc/DB9K-GW3N].

121. Rosenblum, *supra* note 88.

122. *TRUSTe Privacy Index: 2015 Consumer Confidence Edition*, TRUSTE (2015), https://www.truste.com/resources/privacy-research/us-consumer-confidence-index-2015 [https://perma.cc/D4H2-Y72Y] (noting these year-over-year changes under the heading "Consumer Trust").

123. RAINIE & DUGGAN, *supra* note 91, at 3.

124. *See* Rose, *supra* note 109, at 21–22 (discussing how system costs can add greatly to the cost of a Property approach).

The digital trust resource is likely at a point of low-to-medium pressure. Under Rose's typology, this suggests either a *Keepout* or a *Rightway* strategy. *Keepout* is problematic in this context. The information economy thrives on innovation. A regulatory strategy that allowed existing businesses to employ personal information, but prevented new ones from doing so, could seriously hamper the start-ups that provide the sector with so much of its energy and creativity. A *Keepout* strategy might also run afoul of the First Amendment by limiting certain companies' ability to collect and use personal information.[125] *Keepout* fits the digital economy far less well than it fits a fishery.

This leaves us with *Rightway*, a strategy suited to low-to-medium pressure that is more compatible with the information economy. *Rightway* "prescrib[es] the methods by which users may take the resource."[126] With respect to Rose's hypothetical fishers, this might consist of rules specifying that certain types of fishing methods were allowed while others, which could over-use the resource and cause the fish population to crash, were not. In the present case, it would involve rules as to which methods of collecting and using personal information, and so of exploiting user trust, were acceptable, and which were not. The rules would seek to prevent those business activities (such as cell phone flashlight apps that surreptitiously collect contact lists, photos and location information) that could over-exploit user trust and cause it to crash. A *Rightway* strategy could help to preserve sufficient user trust and make the information economy more sustainable in the long term. If the rules applied equally, the *Rightway* approach would not create the barriers to entry that the *Keepout* method is expressly designed to establish.

The picture is not all rosy with respect to *Rightway*, however. The administrative costs of identifying the right way for each relevant sector to collect and use personal information would be high. So would the costs to the regulated businesses (the "user costs," in Rose's terminology). Both sorts of costs would be especially high if the system were set up so that the regulators, rather than the companies themselves, determined which practice or technology was the "right" one for a given industry. The design questions that

125. *Cf.* Sorrell v. IMS Health, Inc., 131 S. Ct. 2653 (2011) (applying heightened judicial scrutiny to a restriction on the sale, disclosure, and use of pharmacy records under free-speech grounds).

126. Rose, *supra* note 109, at 9.

frequently arise with respect to such regulatory systems would rear their heads here as well. Should the standards be arrived at through government rulemaking, industry self-regulation, or a co-regulatory approach that combines the two?[127] What form should these rules take? Should they consist of design standards that tell firms what practices and technologies to use, or performance standards that set an enforceable goal but allow the regulated businesses to figure out how best to achieve it?[128] Do information-based rules that require companies to collect and report certain data about their operations,[129] or management-based standards that require companies to adopt certain internal-management processes,[130] have a role to play? Where are prescriptive standards needed, and where would market-based approaches be more effective?

The major policy issues in the privacy area are, in large part, a variant of these questions. Policymakers and stakeholders have struggled for years over whether industry self-regulation, or direct government regulation, would more effectively and efficiently protect personal information from abuse.[131] The Obama Administration's proposed 2015 Consumer Privacy Bill of Rights Act devotes an entire Title to co-regulatory codes of conduct.[132] The debate between those who defend the notice- and choice-based approach to privacy regulation,[133] and those who prefer a harm-based approach,[134] is in

127. *See, e.g.*, Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation*, 34 SEATTLE U. L. REV. 439 (2011) (comparing these three regulatory approaches with respect to online privacy).

128. *See generally* ROBERT V. PERCIVAL, CHRISTOPHER H. SCHROEDER, ALAN S. MILLER & JAMES P. LEAPE, ENVIRONMENTAL REGULATION: LAW, SCIENCE, AND POLICY 155 (7th ed. 2013) (defining these two types of regulatory standards); Cary Coglianese, Jennifer Nash & Todd Olmstead, *Performance-Based Regulation: Prospects and Limitations in Health, Safety and Environmental Protection*, 55 ADMIN. L. REV. 705 (2003) (discussing the difference between these two approaches); Lauren E. Willis, *Performance-Based Consumer Law*, 82 U. CHI. L. REV. 1309 (2015) (describing performance-based approaches to privacy law and other forms of consumer law).

129. *See* STEPHEN M. JOHNSON, ECONOMICS, EQUITY, AND THE ENVIRONMENT 188–235 (2004) (describing laws that require information collection and disclosure).

130. *See* Cary Coglianese & David Lazer, *Management-Based Regulation: Prescribing Private Management to Achieve Public Goals*, 37 L. & SOC'Y REV. 691 (2003) (exploring this form of regulation).

131. *See id.* at 451–59 (describing the opposing views).

132. THE WHITE HOUSE, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT (2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [https://perma.cc/4AC6-H8YJ].

133. *See, e.g.*, M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2012) (discussing innovative ways to provide notice).

many respects a discussion about whether to employ design standards or performance standards. Regulations that require firms to give specific types of notice in particular ways are a type of design requirement. A standard that called upon companies to avoid certain types or levels of harm, but left it up to the businesses to figure out how to achieve this, would be a performance standard. There are other alternatives as well. State legislatures employ an information-based approach when they pass data security breach notification laws. The FTC employs a management-based approach when it requires companies that have violated the FTC Act to adopt comprehensive privacy-management practices as a condition of settlement. Policymakers, advocates and scholars are, in many respects, already considering which way to regulate is the "Rightway."

This article does not seek to answer this question. Instead, it suggests that these discussions represent nascent efforts to manage the trust commons so as to preserve better this essential resource. If policymakers and stakeholders can identify effective strategies for preventing the abuse of user trust—and if they can combine them with Fairfield and Engel's recommendations for reducing the privacy externalities that individuals create—we might yet avert the tragedy, create the kind of privacy-protective society that many of us want to live in, and lay the groundwork for a prosperous and sustainable information economy.

134. *See, e.g.*, Ctr. for Info. Policy Leadership, A Risk-Based Approach to Privacy? (Mar. 20, 2014) (unpublished manuscript), https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Centres_Privacy_Risk_Framework_Workshop_I_Initial_Issues_Paper.pdf [https://perma.cc/K9JS-NCDM] (encouraging discussion of a more risk-based approach to privacy regulation).