Duke Law Journal

VOLUME 65 DECEMBER 2015 NUMBER 3

PRIVACY AS A PUBLIC GOOD

JOSHUA A.T. FAIRFIELD & CHRISTOPH ENGEL†

ABSTRACT

Privacy is commonly studied as a private good: my personal data is mine to protect and control, and yours is yours. This conception of privacy misses an important component of the policy problem. An individual who is careless with data exposes not only extensive information about herself, but about others as well. The negative externalities imposed on nonconsenting outsiders by such carelessness can be productively studied in terms of welfare economics. If all relevant individuals maximize private benefit, and expect all other relevant individuals to do the same, neoclassical economic theory predicts that society will achieve a suboptimal level of privacy. This prediction holds even if all individuals cherish privacy with the same intensity. As the theoretical literature would have it, the struggle for privacy is destined to become a tragedy.

But according to the experimental public-goods literature, there is hope. Like in real life, people in experiments cooperate in groups at rates well above those predicted by neoclassical theory. Groups can

† Professor of Law, Washington & Lee University School of Law, and Professor Dr., Director, Max Planck Institute for Research on Collective Goods, Bonn, Germany, respectively. Thanks to the participants at the Fourth Annual Internet Works-in-Progress Symposium, the 2014 Telecommunications Policy Research Conference, and workshop participants at the University of Ottawa for comments on drafts of the piece. Thanks in particular to Priscilla Regan, Dennis Hirsch, Chris Jay Hoofnagle, Woody Hartzog, Jane Bambauer, Michael Froomkin, Christopher Seaman, Margaret Hu, Margot Kaminski, Adam Candeub, Jacob Jost, and Greg Lastowka for comments and suggestions. Thanks to Hannah Shtein and Paul Keith for invaluable research support. Thank you to the Fulbright Foundation for support in the original experiments and economic literature review, the Max Planck Institute for Research on Collective Goods for logistical support, and the Frances Lewis Law Center for grant support during the drafting of this article.

be aided in their struggle to produce public goods by institutions, such as communication, framing, or sanction. With these institutions, communities can manage public goods without heavy-handed government intervention. Legal scholarship has not fully engaged this problem in these terms. In this Article, we explain why privacy has aspects of a public good, and we draw lessons from both the theoretical and the empirical literature on public goods to inform the policy discourse on privacy.

TABLE OF CONTENTS

We must all hang together, or assuredly we shall all hang separately.

– Benjamin Franklin

INTRODUCTION

Your privacy is not yours alone. The data that a person produces concerns both herself and others.[1] Being cautious with personal data is therefore not enough. Individuals are vulnerable merely because others have been careless with their data. As a result, privacy protection requires group coordination.[2] Failure of coordination means a failure of privacy. In short, privacy is a public good.

A public good is a social benefit that risks not being produced because everyone can share in it equally, whether they contribute to it or not.[3] In the technical language of economics, a public good is a nonrival and nonexcludable resource.[4] Such goods pose a social dilemma—although society is better off if the good is produced, it is against each individual's best interest to expend resources contributing to the production of the good.[5] Public goods run the gamut, from clean air to national defense.[6] Consumption by one person does not affect consumption by another, and no one can be excluded from consuming.[7] A public bad is the mathematical mirror

1. *See* 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.").

2. *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1927 (2013) ("Privacy rights protect individuals, but to understand privacy simply as an individual right is a mistake. The ability to have, maintain, and manage privacy depends heavily on the attributes of one's social, material, and informational environment.").

3. *See infra* Part II.A; *see also* RICHARD CORNES & TODD SANDLER, THE THEORY OF EXTERNALITIES, PUBLIC GOODS, AND CLUB GOODS 9 (2d ed. 1996) (laying out the general theory of public goods).

4. CORNES & SANDLER, *supra* note 3, at 9 ("The benefits of private goods are fully rival and excludable, whereas the benefits of pure public goods are nonrival and nonexcludable. From the foregoing examples, we see that food and fuel are private, whereas strategic weapons and pollution control are purely public goods.").

5. *Id.*

6. *Id.*

7. *Id.* at 8–9.

image of a public good.[8] A public bad imposes costs, not on any one person, but rather on everyone. Public bads, like polluted water or filthy air, are mathematically identical to public goods, with only the framing of the question differing—are we creating something from which we all benefit (clean air) or avoiding the creation of something that harms everyone (smog)?[9]

An extensive behavioral-economics literature, much of it experimental, focuses on tools that groups can use to solve social dilemmas.[10] Yet that literature has not yet addressed privacy as a public good.[11] The legal literature on privacy suffers from a similar lacuna.[12] Despite many theorists' statements that privacy has an important social dimension,[13] we have found no approach that mines the behavioral or experimental literature for group tools to resist the social dilemma of privacy. This Article fills that gap.

By applying tools from behavioral and experimental economics to the still-intractable legal problem of privacy, we hope to shift the debate surrounding privacy protection. If the theories espoused here are correct, and we believe the science strongly shows they are, the

---

8. Bruce Yandle, *Mixed Goods and Bads*, 19 PUB. CHOICE 95, 95–96 (1974); Kenneth R. Richards, *Framing Environmental Policy Instrument Choice*, 10 DUKE ENVTL. L. & POL'Y F. 221, 268 (2000).

9. *See generally* James Andreoni, *Warm-Glow Versus Cold-Prickle: The Effects of Positive and Negative Framing on Cooperation in Experiments*, 110 Q. J. ECON. 1 (1995) (exploring how the framing of outcomes as public goods or bads affects participant choice).

10. This existing body of knowledge is summarized by John O. Ledyard, *Public Goods: A Survey of Experimental Research*, *in* THE HANDBOOK OF EXPERIMENTAL ECONOMICS 111, 141–69 (J.H. Kagel & A.E. Roth eds., Princeton 1995); Ananish Chaudhuri, *Sustaining Cooperation in Laboratory Public Goods Experiments: A Selective Survey of the Literature*, 14 EXPERIMENTAL ECON. 47, 47–83 (2011); Jennifer Zelmer, *Linear Public Goods Experiments: A Meta-Analysis*, 6 EXPERIMENTAL ECON. 299, 304–07 (2003).

11. *See generally* Andrew F. Daughety & Jennifer F. Reinganum, *Public Goods, Social Pressure, and the Choice Between Privacy and Publicity*, 2 AM. ECON. J. MICROECONOMICS 191 (2010) (modeling a different situation in which contributing to a public good sends a signal about its type that would be individually profitable to keep confidential); Richard Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405 (1981) (comparing an individual's demands for privacy with a seller's demands to conceal product defects and theorizing that the protection of privacy is economically inefficient); Stefan Dodds, *Privacy and Endogenous Monitoring Choice when Private Information is a Public Good* (Queen's Univ. Econ. Dep't, Working Paper No. 1010, 2002), http://qed.econ.queensu.ca/working_papers/papers/qed_wp_1010.pdf [http://perma.cc/SVT9-ZXC2] (focusing on the opposite case where sharing the information is individually detrimental but socially beneficial).

12. *See infra* Parts I.C–D; *see also* MacCarthy, *supra* note 1, at 429 ("[T]here has not been sufficient attention paid to the idea that certain contexts of information disclosure and data analytics can reveal information about people other than the data subject.").

13. *See infra* Part I.D.

manner in which law addresses privacy will and must undergo a sea change. Today's social, legal, and self-regulatory tools focus on empowering individuals. They must equally be focused on empowering groups.

Individual empowerment is not enough because an individual's disclosure of information about herself impacts many other people. One source of risk is immediate and palpable—information about one person is also information about others.[14] If a machine learning algorithm knows where someone is at a given time, it can predict where a spouse or friend is as well. Another source of risk is remote and concealed, but potentially even more dangerous. Big data companies collect large amounts of information about everyone.[15] They then mine this data for patterns.[16] A single cue may facilitate an inference regarding information an individual has chosen not to reveal, or perhaps even something she did not know about herself. For instance, imagine paying higher insurance premiums because a sibling has cancer, or because a parent posts something about his heart disease, or a relative self-identifies as suffering from a particular mental illness.[17] Alternatively, imagine not receiving a job offer because an algorithm has identified that the distance an employee lives from work strongly correlates with higher turnover.[18]

The single-cue examples presented above are only the tip of the iceberg. The true power of big data rests on combining arrays of information.[19] Consider Facebook, which recently applied for a patent

14. *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1939 (2013) ("Big Data is notable not just because of the amount of personal information that can be processed, but because of the ways data in one area can be linked to other areas and produce new inferences and findings.").

15. *See* MacCarthy, *supra* note 1, at 431 ("[T]he biggest dangers associated with online behavioral advertising might come from the possible secondary use of the profiles and analytics constructed to enable targeted advertising.").

16. *See* Richards, *supra* note 14, at 1939 ("Big Data is fundamentally networked. Its value comes from the patterns that can be derived by making connections between pieces of data, about an individual, about individuals in relation to others, about groups of people, or simply about the structure of information itself."); Jordan Ellenberg, *What's Even Creepier than Target Guessing that You're Pregnant?*, SLATE: HOW NOT TO BE WRONG (June 9, 2014), http://www.slate.com/blogs/how_not_to_be_wrong/2014/06/09/big_data_what_s_even_creepier_than_target_guessing_that_you_re_pregnant.html [http://perma.cc/E68S-UP4C].

17. *See* MacCarthy, *supra* note 1, at 450 ("If a data collector knows the independent variable in that circumstance, it can use the regularity to infer the presence of the dependent variable, even when the people involved have not revealed the presence of that characteristic and it cannot be found in public records.").

18. *See id.* at 450–51 (discussing how big data impacts eligibility decisions).

19. *See* Richards, *supra* note 14.

for inferring the creditworthiness of an individual based on the financial responsibility of the people in that individual's social network.[20] Each person's financial decisions feed into the algorithm's decisions about whether to extend others a loan.[21] Moreover, the array of cues that might play into the determination of each individual's financial responsibility (or any other attribute) can be vast and of varying precision. Sometimes a combination of cues is so tightly related to the unobserved information that it gives rise to a strong inference. For example, one study demonstrated that 87 percent of the U.S. population can be uniquely identified just from zip code, gender, and date of birth.[22] In some instances the inference might be wrong,[23] but those relying on the cue pattern often do not care because they can afford to err on the side of caution.[24] For example, an insurance company may prefer to lose a few customers rather than insure individuals whose relationships indicate a greater likelihood of expensive genetically linked illness.

Individual control of data is a fundamentally flawed concept because individuals cannot know what the data they reveal means when aggregated with billions of other data points. For example, people who buy felt pads for their furniture are more likely to pay back loans because they are conscientious with their belongings; people who log into their credit-card accounts at 1:00 a.m. may be showing signs of financial anxiety; and people who use credit cards at drinking establishments are more likely to default on loans than people who use credit cards at the dentist.[25] Big data firms learn these things by gathering colossal datasets from millions of people and

20. *See* Susie Cagle, *Facebook Wants to Redline Your Friends List*, PAC. STANDARD MAG. (Aug. 24, 2015), http://www.psmag.com/nature-and-technology/mo-friends-mo-problems-might-have-to-defriend-joey-with-the-jet-ski-bankruptcy [http://perma.cc/TY87-MBBF].

21. *Id.* ("In short: You could be denied a loan simply because your friends have defaulted on theirs. It's the kind of digital redlining that critics of 'big data' collection have been warning of for years.").

22. *See* LATANYA SWEENEY, CARNEGIE MELLON UNIV., SCHOOL OF COMP. SCI., DATA PRIVACY LAB., RE-IDENTIFICATION OF DE-IDENTIFIED SURVEY DATA (2000).

23. *See* Tim Harford, *Big Data: Are We Making a Big Mistake?*, FIN. TIMES (Mar. 28, 2014), http://www.ft.com/cms/s/2/21a6e7d8-b479-11e3-a09a-00144feabdc0.html [http://perma.cc/HMR8-WHPD] (detailing the problem of attributing cause to highly correlated data points in found datasets).

24. *See* MacCarthy, *supra* note 1, at 455 ("These indirect disclosures are usually probabilistic rather than certain.").

25. Charles Duhigg, *What Does Your Credit Card Company Know About You?*, N.Y. TIMES MAG. (May 12, 2009), http://www.nytimes.com/2009/05/17/magazine/17credit-t.html?pagewanted=all&_r=0 [http://perma.cc/E2W2-VPY8].

mining the resulting pools of information. No matter how healthy or creditworthy or committed to work a person may be, he might not receive a home loan, job offer, or affordable insurance, because of correlations ascertained from others' data.

If you believe in the effectiveness of incentivizing, informing, and empowering individual citizens to protect their own privacy, this is very bad news. As long as the immediate benefit from disclosing your data exceeds the ensuing long-term risk for your own privacy, you will give away your data. This prediction holds even if all individuals cherish privacy with the same intensity. If neoclassical economic theory is correct, the struggle for privacy is destined to become a tragedy.[26]

But all hope is not lost. Both in the field and under the tightly controlled conditions of a lab, groups have effectively produced public goods.[27] The tragedy can be overcome. Good will alone, however, is not enough. Instead, group rules or structural conditions (called "institutions") must trigger and channel contributors' sense of altruism and equity.[28] This works even better if an institution actively foments cooperation.[29] Luckily, privacy is by no means the only public good. Clean air, safety, roads, and the common defense all share the same incentive structure.[30] Privacy policy thus need not reinvent the

---

26. *See generally* Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243 (1968) (theorizing that when given a choice, individuals will act in a way that is beneficial to themselves, even though the collective actions of all such individuals will be detrimental both to themselves and society as a whole). For an application to privacy and information, see Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 10 (2006) [hereinafter Hirsch, *Inner Environment*] ("Privacy injuries, much like environmental damage, accordingly qualify as 'negative externalities.' If left unchecked, these privacy-infringing industries will ultimately destroy the very resources on which they themselves depend. This will generate the same kind of 'tragedy of the commons' that environmental laws were designed to alleviate.").

27. *See, e.g.*, Ledyard, *supra* note 10, at 121 (noting that people do make contributions to the public good, that "[f]ace to face communication improves the rate of contribution," and that "the public goods problem is not as bad as some economists make it out to be").

28. *See* Andreoni, *supra* note 9, at 13 ("[C]ooperation in public goods experiments cannot be explained by pure altruism that subjects may have for each other. . . . Instead there must be some asymmetry in the way people feel personally about doing good for others versus not doing bad: the warm-glow must be stronger than the cold-prickle.").

29. *See, e.g.*, James Andreoni & Larry Samuelson, *Building Rational Cooperation*, 127 J. ECON. THEORY 117, 122 (2006) ("A player thus prefers that his opponent cooperate, and finds cooperation relatively more attractive the more likely is the opponent to cooperate.").

30. *See, e.g.*, CORNES & SANDLER, *supra* note 3, at 517 ("The selling price differential between two houses whose characteristics are the same except for air quality provides a measure for the private willingness to pay for the public good of clean air."); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2084–85 (2004) [hereinafter

wheel; it can benefit from solutions developed and tested in these areas. From this perspective, privacy is no longer a tragedy, but it remains a drama, calling for vigilance and, ideally, intervention in the form of group-empowering institutions that enable sustained cooperation in the face of a social dilemma.[31]

Inattention to privacy's public-good nature has led privacy policy astray.[32] In the absence of public-policy attention to privacy's group dimension, individual consumers have been left to negotiate, unsuccessfully, with companies over the use of their data. Private companies have accumulated deep and potentially toxic pools of consumer data, and have made this data available to governments with few legal safeguards.[33] Social-media networks have become the business end of dragnet surveillance.[34] The transition to mobile computing and its attendant geolocation data exacerbates the problem.[35] Systems designed to use geolocation to deliver

---

Schwartz, *Property*] ("From this perspective, information privacy functions as a type of public good, like clean air or national defense.").

31. *See* COMM. ON THE HUMAN DIMENSIONS OF GLOBAL CHANGE, NAT'L RESEARCH COUNCIL, THE DRAMA OF THE COMMONS (Elinor Ostrom et al. eds., National Academy Press 2002) [hereinafter DRAMA].

32. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 266–69 (2011).

33. *See* Tom Hamburger, *Privacy Rights Need Urgent Protection in Washington, Activists Say*, WASH. POST (Feb. 24, 2014), http://www.washingtonpost.com/politics/consumer-privacy-rights-need-urgent-protection-in-washington-activists-say/2014/02/24/1764ba22-9cb7-11e3-975d-107dfef7b668_story.html [http://perma.cc/QG8M-W3JV] ("Privacy protection demands have increased in recent months as data-collection companies face new pressure from European regulators alarmed by disclosure of U.S. government spying."); Bruce Schneier, *The Tech Lab: Bruce Schneier*, BBC (Feb. 26, 2009), http://news.bbc.co.uk/2/hi/technology/7897892.stm [http://perma.cc/FJA8-GBVA] ("Data is the pollution of the information age. It's a natural by-product of every computer-mediated interaction. It stays around forever, unless it's disposed of. It is valuable when reused, but it must be done carefully. Otherwise, its after-effects are toxic. And just as 100 years ago people ignored pollution in our rush to build the Industrial Age, today we're ignoring data in our rush to build the Information Age.").

34. *See* Bruce Schneier, *Don't Listen to Google and Facebook: The Public-Private Surveillance Partnership is Still Going Strong*, THE ATLANTIC (Mar. 25, 2014, 11:08 AM), http://www.theatlantic.com/technology/archive/2014/03/don-t-listen-to-google-and-facebook-the-public-private-surveillance-partnership-is-still-going-strong/284612 [http://perma.cc/M8PE-ZBCJ] ("Google, and by extension, the U.S. government, still has access to your communications on Google's servers.").

35. *See* Brian Fung, *Verizon Transparency Report Reveals 320,000 Data Requests in 2013*, WASH. POST: THE SWITCH (Jan. 22, 2014, 12:17 PM), http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/22/verizon-transparency-report-reveals-320000-data-requests-in-2013 [http://perma.cc/YRZ4-ENG4].

advertisements to mobile devices serve as tools of political oppression.[36]

Policymakers must change tack to effectively moderate this trend. Well-meaning legislators, judges, and regulators have focused almost exclusively on two elements: individual consumer comprehension (notice), and individualized control (choice).[37] We support these efforts, but believe that other approaches offer greater value, in particular approaches that arm groups against social dilemmas.

This Article starts that conversation and provides some framing principles to promote collective action on privacy. We take seriously the as-yet unanswered call for more extensive study of privacy as a public good.[38] We further think that the behavioral-economics literature—which asks how people actually behave in these situations—draws a clearer picture than the excessively rigorous pure-theory public goods of neoclassical economics.[39]

In neoclassical economics, a dilemma results from a difference between individual and social benefit.[40] The individual is best off if

---

36. *See* Andrew E. Kramer, *Ukraine's Opposition Says Government Stirs Violence*, N.Y. TIMES (Jan 22, 2014), http://www.nytimes.com/2014/01/22/world/europe/ukraine-protests.html [http://perma.cc/D2VJ-364C] (detailing the use of cell phone site location technology to deliver threats to protesters).

37. *See* Press Release, The White House, Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights (Feb. 23, 2012), https://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b [https://perma.cc/83CJ-JZLV]; Jennifer Martinez, *Markey Introduces Mobile Privacy Bill*, THE HILL (Sept. 12, 2012, 5:46 PM), http://thehill.com/policy/technology/249055-markey-introduces-mobile-privacy-bill [http://perma.cc/JG4Y-MNKJ]; Somini Sengupta, *Web Privacy Becomes a Business Imperative*, N.Y. TIMES (Mar. 3, 2013), http://www.nytimes.com/2013/03/04/technology/amid-do-not-track-effort-web-companies-race-to-look-privacy-friendly.html?page wanted=all [http://perma.cc/N7GH-3HDP] ("Privacy is no longer just a regulatory headache. Increasingly, Internet companies are pushing each other to prove to consumers that their data is safe and in their control.").

38. *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 228, 231 (1995) ("Recognition that privacy has some features of a public or collective good would make clearer the institutional or organizational interests in personal information and the weaknesses of a market solution in providing privacy protection.").

39. *See* Christine Jolls, Cass R. Sunstein & Richard Thaler, *A Behavioral Approach to Law and Economics*, 50 STAN. L. REV. 1471, 1473 (1998) (suggesting incorporating behavioral economics into law and economics and noting that "[t]he absence of sustained and comprehensive economic analysis of legal rules from a perspective informed by insights about actual human behavior makes for a significant contrast with many other fields of economics, where such 'behavioral' analysis has become relatively common").

40. *See* Richard Warner & Robert H. Sloan, *Behavioral Advertising: From One-Sided Chicken to Informational Norms*, 15 VAND. J. ENT. & TECH. L. 49, 55 (2012) ("Collective action

she ignores the negative or positive effects that her action entails for others.[41] This holds even if the individual foresees that all other relevant outsiders will behave the same way.[42] She then foresees that she will suffer severely from others' inflicting harm on her, or withholding socially desirable behavior.[43] Even so, if she is the only one to take the ramifications of her actions on others into account, she will be even worse off. Others would suffer a little less, or they would gain a little, but she would experience less benefit than all other selfish individuals would enjoy collectively.[44] If she expects all others to be selfish, she has no incentive to consider the common good herself.[45]

The neoclassical literature therefore supposes that individually informed and empowered actors will act against group social welfare.[46] But experimental literature shows repeatedly that the neoclassical picture is too pessimistic. A rich literature[47] has tested and rejected the theoretical prediction that groups will completely fail to produce public goods.[48]

---

problems are situations in which everyone is worse off if everyone does what he individually prefers to do.").

41. *Id.*

42. *See* Margaret M. Blair & Lynn A. Stout, *Trust, Trustworthiness, and the Behavioral Foundations of Corporate Law*, 149 U. PA. L. REV. 1735, 1765–66 (2001) (discussing how trustworthy people expect others to also be trustworthy, and vice versa).

43. *See id*.

44. *See id*.

45. *See id*.

46. *See id.* at 1751 (noting that the neoclassical model is one of "human behavior driven by rational self-interest"); Jennifer L. Radner, *Phone, Fax, and Frustration: Electronic Commercial Speech and Nuisance Law*, 42 EMORY L.J. 359, 404–05 (1993) ("Further, the [neoclassical] model assumes that individuals are able to accurately judge their own welfare and that their decisions will not be dependent upon the welfare of others."); *see generally* CORNES & SANDLER, *supra* note 3 (presenting a theoretical framework of externalities); TODD SANDLER, GLOBAL COLLECTIVE ACTION (2004) (analyzing factors that affect the success or failure of collective action); TODD SANDLER, COLLECTIVE ACTION: THEORY AND APPLICATION (1992) (providing a summary of collective-action research); Hardin, *supra* note 26 (introducing Hardin's well-known theory).

47. Surveys are provided by Chaudhuri, *supra* note 10, at 56–59; Ledyard, *supra* note 10, at 111; and Zelmer, *supra* note 10, at 304–08.

48. *See, e.g.*, Robert J. Aumann & Lloyd S. Shapley, *Long Term Competition—A Game Theoretic Analysis*, *in* COLLECTED PAPERS: R.J. AUMANN 395, 396 (1992) (concluding that "individual self-interest in [certain] situations can in fact dictate a kind of cooperative behavior"); David M. Kreps, Paul Milgrom, John Roberts & Robert Wilson, *Rational Cooperation in the Finitely Repeated Prisoners' Dilemma*, 27 J. ECON. THEORY 245, 245–52 (1982) (presenting "how reputation effects due to informational asymmetries can generate cooperative behavior in finitely repeated versions of the classic prisoners' dilemma"); Reinhard

When humans enter the lab, they resist public-goods problems and attempt to cooperate at rates well above that which theory would predict.[49] They struggle.[50] Often, given the math of the experiments, they are doomed to ultimate failure, but they struggle nonetheless. Different features of the collective-action environment mean that their struggles have more or less success.[51] Following Nobel Prize winner Elinor Ostrom, we term this struggle the drama of the commons.[52] If game theory were entirely correct, a community facing a problem that has the properties of a public good would be doomed to tragedy. The community would suffer maximum damage. Luckily both in the lab[53] and in the field this prediction is too gloomy.[54] Some communities in some contexts have found viable and sustainable ways to overcome the dilemma.

Consequently, groups must be given tools to create the public good of privacy and resist the public bad of readily available intrusive information (which one might call "data pollution"). Informing and empowering individual players does not resolve a social dilemma. It is precisely the fully informed, rational, and empowered individual who knows she is better off contributing fully to a public bad, and free riding on a public good, regardless of the actions of others.[55] The relevant legal tools therefore should be redesigned to focus less on

---

Selten, *The Chain Store Paradox*, 9 THEORY & DECISION 127, 127–59 (1978) (presenting three levels of individual decisionmaking that help to refute basic game-theory assumptions).

49. *See* Blair & Stout, *supra* note 42, at 1761 ("[I]ndividuals in social dilemma experiments exhibit far more cooperative behavior than can possibly be explained by external incentives.").

50. *See id.* at 1761–62 (noting that individuals essentially show two personalities in experimental social-dilemma contexts, and "[w]hen the competitive personality is dominant, an individual will choose options that maximize her personal payoffs without regard for effects on others . . . [and w]hen the cooperative personality governs, an individual will choose options that maximize group welfare over options that maximize her own").

51. *See id.* at 1768 ("[A] . . . key empirical finding from the social dilemma studies is that even high trusters, in the right circumstances, predictably choose to defect rather than cooperate. The key appears to be whether, when faced with a new situation that presents social dilemma payoffs, an individual categorizes it as a *competitive* task or a *cooperative* task.").

52. *See* DRAMA, *supra* note 31, at 4.

53. *See supra* notes 47–48 and accompanying text.

54. *See* ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION 1 (1990) ("[C]ommunities of individuals have relied on institutions resembling neither the state nor the market to govern some resource systems with reasonable degrees of success over long periods of time.").

55. *See* Robyn M. Dawes & Richard H. Thaler, *Anomalies: Cooperation*, 1988 J. ECON. PERSP. 187, 196 ("Perhaps we need to give more attention to 'sensible cooperators.'").

individual knowledge and empowerment and more on facilitating groups' collective protection of their privacy.[56]

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.[57] We suggest positive framing to promote altruism.[58] We suggest that communication and (private) sanctions are key components of group coordination.[59] With these tools, groups may be able to sustain privacy without governmental intervention and the challenges and distortions that flow therefrom.[60]

The balance of this Article proceeds as follows. Part I explains the gap in law and policy by describing first how data mining can cause one person's data to negatively impact others before analyzing why privacy theory has had trouble proposing ways to contain these harms. Part II lays out the case for treating privacy as a public good as strictly defined in the economics literature, and Part III describes methods and tools drawn from the behavioral and theoretical literature that will empower groups to collectively protect privacy.

I. THE GAP IN LAW AND POLICY

Just about every middle schooler understands that a fundamental problem of privacy online is not what one says about oneself, but what others say.[61] Big data exacerbates this problem beyond gossip and thoughtless comments. Big data allows users to reveal critical

---

56. *Cf.* Cohen, *supra* note 2, at 1927.

57. *See* David A. Dana, *Adequacy of Representation After* Stephenson*: A Rawlsian/Behavioral Economics Approach to Class Action Settlements*, 55 EMORY L.J. 279, 303 (2006) (noting the influence of inequality aversion on class-action settlements).

58. *See* Stephanos Bibas, *Plea Bargaining Outside the Shadow of Trial*, 117 HARV. L. REV. 2463, 2512 (2004) ("Options that are packaged as gains (for example, 'lives saved') induce risk aversion; when the very same choices are packaged as losses ('lives lost'), they induce risk taking because of loss aversion.").

59. *See* Richard H. McAdams, *Beyond the Prisoners' Dilemma: Coordination, Game Theory, and Law*, 82 S. CAL. L. REV. 209, 218 (2009) (noting that law serves as a mechanism for cooperation and coordination).

60. *See id.*; Blair & Stout, *supra* note 42, at 1771 ("[A]llowing the players to communicate with each other in a social dilemma significantly increases the incidence of cooperation.").

61. *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1892 (2013) [hereinafter Solove, *Introduction*] ("Additionally, privacy self-management fails to account for the social impacts of individual privacy decisions.").

information about other people without understanding they are doing so.[62] Even by revealing personal interests and disinterests, users train machine-learning algorithms to predict the behavior of other people, forming the basis for targeted behavioral advertising,[63] and creating the potential for abuse by other interested actors.

This Part explores the need for policymakers to fully engage with privacy as a public good. Our specific goals in this Part are to underscore the importance of treating privacy as a social dilemma by showing how the data we share about one another can form toxic pools; to discuss privacy theory's overinvestment in individual-centered theories of privacy; to demonstrate the resulting lacuna in the legal literature on the subject of privacy as a public good as strictly defined by the economics literature; and thus to establish the necessity of our contribution: mining the behavioral- and empirical-economics literature for tools to arm groups against the social dilemma of privacy.

A. Limitations on Scope

Privacy theory has long attempted to define privacy in terms of its core or constitutive elements.[64] We do not take this approach. Rather than seeking to define privacy, we seek to provide tools that help groups minimize the damage caused by information-based social dilemmas. Our approach is consistent with most definitions of privacy, because we suggest not a definition, but a set of institutional features that permit groups to sustain cooperation. Our agnosticism as to any single definition of privacy necessarily colors our approach

62. *See* Terence J. Lau, *Towards Zero Net Presence*, 25 NOTRE DAME J.L. ETHICS & PUB. POL'Y 237, 244 (2011) ("Most users do not realize, however, that the information they post on social media websites can sometimes yield unintended consequences."); MacCarthy, *supra* note 1, at 448 ("[A]n individual's decision to share information with a data collector imposes costs on other individuals. . . . [T]here is leakage of information about individuals who do not themselves choose to reveal it."); Richards, *supra* note 14, at 1939; Solove, *Introduction*, *supra* note 61, at 1881 ("It is virtually impossible for people to weigh the costs and benefits of revealing information or permitting its use or transfer without an understanding of the potential downstream uses, further limiting the effectiveness of the privacy self-management framework.").

63. *See, e.g.*, Riva Richmond, *As 'Like' Buttons Spread, So Do Facebook's Tentacles*, N.Y. TIMES: BITS (Sept. 27, 2011, 3:51 PM), http://bits.blogs.nytimes.com/2011/09/27/as-like-buttons-spread-so-do-facebooks-tentacles/?_php=true&_type=blogs&_r=0 [http://perma.cc/T7DT-TY7C].

64. *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1099–1123 (2002) [hereinafter Solove, *Privacy*] (gathering and challenging essentialist conceptions of privacy).

to the legal literature that attempts to define privacy. We find these attempts to capture the essence of privacy in a definition interesting, but ultimately orthogonal to our approach. We instead offer an approach that may permit groups to protect what they consider to be private at significantly lower cost, and with reduced need for government intervention. The goal is to kick off future debate about the value of continuing with an individual-focused approach to privacy protection. The practical result of this limitation in scope is that we do not believe that adherence to any particular school of thought regarding what privacy is (with the narrow exception of some elements of privacy as individualized control, to which we return below) detracts from the approach advanced here.

A second caveat: information produces both positive and negative network effects, and both positive and negative externalities.[65] This Article takes no position on the upside of information gathering, or on whether the gains from information gathering outweigh the privacy losses. To us, it does not matter: minimizing privacy costs associated with data accumulation is one way to maximize the net gains or reduce the net losses. To provide an example, suppose the government (or Apple, or Google) gathered everyone's healthcare data and parsed it with big data tools. Some people would suffer adverse healthcare decisions (for example, insurance-premium raises, inadequate coverage, and high deductibles) based on this data. Others would benefit from cures we might be able to tease from the mass of correlations. Both can be simultaneously true. Our approach seeks to minimize the downside of this function, not to argue the upside does not exist.

In some situations, individuals will evaluate the same degree of information revelation differently. For example, if I have already been diagnosed with a socially stigmatized illness and am in the hospital, I may not be particularly concerned about this information being used by some online platform. Possibly, all I care about is medicine advancing fast enough to prolong my life. By contrast, others may have a very strong interest in keeping the same piece of information confidential since they fear losing their jobs. Defining the optimal solution for such conflicts resulting from deep heterogeneity is beyond the scope of this Article. Given that privacy as a public

65. *See* Jane R. Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 227 (2012) ("[P]rivacy losses are the negative externalities from an otherwise productive and worthwhile activity—information flow.").

good is not on the scholarly or policymaking radar, we deem it important to first explain why this perspective is often appropriate. We leave it to future work to explore the qualification resulting from deep heterogeneity.

B. Toxic Data Accumulation

Central to our thesis is the idea that large pools of data accumulated over time and from many different sources can exert a corrosive effect on social welfare.[66] Two salient features of accumulated data make it potentially toxic. The first is that data accumulates across time. Humans do not remember contributing the information and do not take precautions against misuse. The second feature is that data accumulates across sources. Again, humans do not adequately account for the fact that what they tell one counterparty will be communicated many times to many others. In both senses, the accumulated data is experienced as toxic: it can harm people in ways they did not foresee.

Because of these effects, security expert Bruce Schneier has called data "the pollution of the information age."[67] Stale data can cause damage because of its privacy impact. For example, assume that because of a youthful indiscretion, an individual received a drug conviction, for which she paid a penalty, or suppose that she had engaged in political protests that create a risk of employer backlash. Decades ago, she could have moved on with her life with confidence that her prior conduct would not come back to haunt her, because the information was not concatenated with other datasets or stored in easily searchable fashion. Now, a conviction results in exclusion from the economy because the information is permanently recorded and spreads into background-check databases. Stale data damages citizens' ability to reinvent themselves; it increases the risk of identity theft; it increases price discrimination;[68] and, through filter bubbling (the practice of limiting search results based on the searching party's data profile),[69] it decreases the ability of citizens to make informed

66. *See id*.

67. *See* Schneier, *supra* note 33.

68. *See* ANNA BERNASEK & D.T. MONGAN, ALL YOU CAN PAY: HOW COMPANIES USE OUR DATA TO EMPTY OUR WALLETS 17–20 (2015).

69. *See generally* ELI PARISER, THE FILTER BUBBLE: WHAT THE INTERNET IS HIDING FROM YOU (2011) (detailing how technology firms influence citizens by limiting search information to personalized results).

choices drawn from a range of data sources, among a number of other potential effects.

We take Schneier's intuition one step further. We ask why groups of people remain willing to continue pouring data into those pools. One stock response, which we find unconvincing, is that people do not care about privacy.[70] The answer we advance here instead is that groups and individuals have different incentives. This answer is particularly elegant: public-goods theory explains why everyone might deeply cherish privacy, yet still contribute to privacy-damaging stores of data, just as everyone likes clean air, but individuals still pollute.

The truth of Schneier's suggestion has been repeatedly demonstrated in the field. In 2006, AOL Inc. (AOL) released twenty million search queries to researchers.[71] Privacy organizations termed this event a "data Valdez," a reference to the oil spill caused by a run-aground tanker off the Alaskan coast.[72] Yet just as the original Valdez spill now appears tiny compared to subsequent breaches such as the British Petroleum spill, so subsequent data breaches have made AOL's search leak seem miniscule in comparison.[73] The leaks have grown in size and potential financial damage. Malware residing on Home Depot cash registers captured the credit information of fifty-six million card holders in September 2014.[74] Another hack involved 160 million credit-card and debit-card numbers, stolen over a seven-year

70. *See, e.g.*, Greg Satell, *Let's Face It, We Don't Really Care About Privacy*, FORBES (Dec. 1, 2014), http://www.forbes.com/sites/gregsatell/2014/12/01/lets-face-it-we-dont-really-care-about-privacy [http://perma.cc/R27Y-6485] (characterizing a Pew survey indicating that 91 percent of Americans feel "that consumers have lost control over how personal information is collected and used by companies" as evidence that although Americans are aware of personal monitoring, they do not do enough to stop it).

71. Michael Barbaro & Tom Zeller, Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES (Aug. 9, 2006), http://www.nytimes.com/2006/08/09/technology/09aol.html?page wanted=all [http://perma.cc/N4UB-X782].

72. *See, e.g.*, Derek Slater, *AOL's Data Valdez Violates Users' Privacy*, ELEC. FRONTIER FOUND. (Aug. 7, 2006), https://www.eff.org/deeplinks/2006/08/aols-data-valdez-violates-users-privacy [http://perma.cc/5LE2-AVCF].

73. *See, e.g.*, Brian Fung, *The Target Hack Gets Worse: Phone Numbers, Addresses of Up to 70 Million Customers Leaked*, WASH. POST: THE SWITCH (Jan. 10, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/10/the-target-hack-gets-worse-phone-numbers-addresses-of-up-to-70-million-customers-leaked [http://perma.cc/6ER4-3XLA] (documenting the data breach of Target, compromising the data of 70 million people).

74. *See* Jim Finkle & Nandita Bose, *Home Depot Breach Bigger than Target at 56 Million Cards*, REUTERS (Sept. 18, 2014, 7:16 PM), http://www.reuters.com/ article/2014/09/18/us-home-depot-dataprotection-idUSKBN0HD2J420140918 [http://perma.cc/6FBX-PDWX].

period.[75] Hacks of tens of millions of cards from major retailers came to light during the 2013 holiday season.[76] These hacks were augmented by the theft of non-credit-card private information gathered from seventy million customers, including names, addresses, email addresses, and phone numbers.[77] The U.S. Office of Personnel Management suffered a serious hack in which the personal data of over twenty million people was compromised.[78] Hacks are increasing in frequency and impact because the pools of data stored by companies continue to grow.[79] Because more data can be compromised in a single leak, hackers have a greater incentive to instigate such a leak. As a result, merely accumulating data in connection with regular e-commerce creates a toxic buildup of incentives to steal and misuse that data.

Consumer-credit hacks are just the tip of the iceberg. Social media provides rich troves for data researchers.[80] Users disclose data about shops they visit, trips they take, routes they drive, food they eat, and increasingly people they encounter.[81] Users tag photographs of one another on Facebook.[82] Users reference one another in geolocated social-media posts. They comment on one another's

75. Daniel Beekman, *Hackers Hit Companies Like Nasdaq, 7-Eleven for $300 Million, Prosecutors Say*, NY DAILY NEWS (July 26, 2013, 12:41 PM), http://www.nydailynews.com/news/national/russians-ukrainian-charged-largest-hacking-spree-u-s-history-article-1.1408948 [http://perma.cc/3GM5-Y88K].

76. *See* Gregory Wallace, *Target and Neiman Marcus Hacks: The Latest*, CNN MONEY (Jan. 13, 2014, 12:35 PM), http://money.cnn.com/2014/01/13/news/target-neiman-marcus-hack [http://perma.cc/LU8J-FQ2X].

77. *See id*.

78. *See* David Jackson & Kevin Johnson, *China Suspected in Massive U.S. Government Data Breach*, USA TODAY (June 5, 2015, 12:42 PM), http://www.usatoday.com/story/news/nation/2015/06/04/obama-office-of-personnel-management-data-breach/28495775 [http://perma.cc/H2DQ-MGSZ] (noting that the recent data theft from the Office of Personnel Management computer systems compromised sensitive personal information, including Social Security numbers, credit-card data, and other forms of financial information of roughly 21.5 million people from both inside and outside the government).

79. *See* Martin Hilbert & Priscila López, *The World's Technological Capacity to Store, Communicate, and Compute Information*, 332 SCIENCE 60, 63–64 (2011) (detailing geometric increase in worldwide data-storage capacity).

80. *See* Michael Birnhack, *Reverse Engineering Informational Privacy Law*, 15 YALE J.L. & TECH. 24, 85 (2013) ("[N]ew network applications, especially social networks, enable (or perhaps push) users to share personal data.").

81. *See id*. at 86.

82. *See* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1145–46 (2009) ("There's a photo-sharing feature, imaginatively names 'Photos,' with a clever tagging system: click on a face in a photo—even one posted by someone else—and you can enter the person's name.").

walls.[83] They take photographs of one another with Snapchat, and post commented pictures to Instagram.[84] Consumers do this in the mistaken belief that data is ephemeral, or because of too-often-broken promises that consumer data can be kept safe from other consumers or malicious third parties.[85]

Ubiquitous smartphones permit users to contribute data about themselves and others on a constant basis.[86] People have fewer places to hide from social-media-enabled computing because others carry it with them.[87] There are vanishingly few modern social situations in which no one in the room is carrying a GPS-embedded or voice-activated device. Engaging with social media is therefore not an individual choice. It is an inevitable outcome of being in almost any social situation. Location information is a particularly powerful example of how one person's data can affect others. Cell phones track individuals' location precisely, and by proxy, the locations of others.[88]

---

83. *See* Jason Mazzone, *Facebook's Afterlife*, 90 N.C. L. REV. 1643, 1653 (2012) ("Facebook users do not necessarily want those responses and comments associated with their own individual accounts, and therefore themselves, to be publicly accessible.").

84. *See* Nick Bilton, *Disruptions: Indiscreet Photos, Glimpsed Then Gone*, N.Y. TIMES: BITS (May 6, 2012, 5:24 PM), http://bits.blogs.nytimes.com/2012/05/06/disruptions-indiscreet-photos-glimpsed-then-gone [https://perma.cc/4NS8-9YGK]; Josh Constine, *Instagram Now Lets Anyone Tag You [Or Brands] In Photos, Adds Them To "Photos of You" Profile Section*, TECHCRUNCH (May 2, 2013), http://techcrunch.com/2013/05/02/instagram-photo-tagging [http://perma.cc/7FR7-SLJE].

85. *See* Catherine Shu, *Confirmed: Snapchat Hack Not A Hoax, 4.6M Usernames And Numbers Published*, TECHCRUNCH (Dec. 31, 2013), http://techcrunch.com/2013/12/31/hackers-claim-to-publish-list-of-4-6m-snapchat-usernames-and-numbers [http://perma.cc/H3GR-59VH] (noting that two data breaches at Snapchat "are both reminders that even in an ephemeral messaging service, it would be a mistake to be lulled into a sense of security about the information that you do have stored with the app"); *see also* Press Release, Federal Trade Commission, Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False (May 18, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were [https://perma.cc/2FS4-TJDA].

86. *See* Thomas H. Chia, *Fighting the Smartphone Patent War with Rand-Encumbered Patents*, 27 BERKELEY TECH. L.J. 209, 231 (2012) (discussing how smartphone operating systems' data collection can lead to increased probability of a monopoly).

87. *See* Peter Swire, *Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment*, 90 N.C. L. REV. 1371, 1381–82 (2012) (noting that privacy is once again a salient issue given, in part, both the "rise of social networks" and the "skyrocketing use of mobile devices").

88. *See* Lau, *supra* note 62, at 245 (noting the existence of "a new generation of social networking built upon wireless platforms with Global Position System (GPS) technology"); *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-903, MOBILE DEVICE LOCATION DATA: ADDITIONAL FEDERAL ACTIONS COULD HELP PROTECT CONSUMER PRIVACY 11–13 (2012) (noting that "[s]ince the advent of consumer cellular technology, making and receiving mobile

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.[89]

Users have accepted a far more invasive set of end-use license conditions governing their use of smartphones than they have for desktops and laptops.[90] These smartphone contracts are understood and construed as agreements purely between the consumer and the carrier, operating-system designer, manufacturer, or application provider. Data disclosed under these agreements impacts third parties who have no say. Users' contact lists and personal calendars are regularly scraped by mobile applications.[91] Users' email conversations with nonconsenting third parties are parsed by their email services.[92] Carriers hide keystroke-logging software on cell phones, and append tracking IDs to outgoing connections, so that consumers are comprehensively tracked without their knowledge.[93] Browsing activity can then be combined with geolocation and social-media mapping to

telephone calls has depended on the ability to determine a device's location" and that new location-tracking technologies have made it easier to track location).

89. *See* James Risen & Laura Poitras, *NSA Gathers Data on Social Connections of U.S. Citizens*, N.Y. TIMES (Sept. 28, 2013), http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=all&_r=0 [http://perma.cc/B7SP-TS2F] (discussing the National Security Agency's use of social connections to track a target's locations, relationships, and other personal data).

90. *See* Lau, *supra* note 62, at 251–52 ("As a customer uses [Google's G1 phone], data such as the user's name, contacts, instant messages, emails, calendars, social networking site visits, and videos downloaded are all collected. The user cannot see what specific data is collected, and there is no way to expunge the data.").

91. *See, e.g.*, Geoffrey A. Fowler, *Secrets You Share Online Aren't Always So Secret*, WALL ST. J. (Feb. 25, 2014, 7:54 PM), http://www.wsj.com/articles/SB10001424052702303880604579405020639967010 [http://perma.cc/WQ3Z-PVBF] (describing secret-posting apps that "peddle anonymity, [but] collect enough information to build profiles about each user," for instance by "tapping . . . location and contacts to share [postings] anonymously with [existing contacts]").

92. *See* Eben Moglen, Address at Columbia Law School, Snowden and the Future: Part III; The Union, May It Be Preserved (Nov. 13, 2013), http://snowdenandthefuture.info/snowdenandthefuture-unionpreserved.pdf [http://perma.cc/3TEN-EUZL].

93. *See* Andrew D. Salek-Raham, *Carrier IQ, Pre-Transit Keystroke Logging, and the Federal Wiretap Act*, 13 N.C. J.L. & TECH. 417, 426 (2012) (describing use of "embedded handset software that automatically provides real-time data . . . without requiring user participation or knowledge"); Robert McMillan, *Verizon's Perma-Cookie is a Privacy Killing Machine*, WIRED (Oct. 27, 2014, 6:30 AM), http://www.wired.com/2014/10/verizons-perma-cookie [http://perma.cc/T8PD-3DF6] (describing Verizon's process of appending a UIDH to customers' web traffic).

provide a total profile of the user, her social network, her real-world location, and her interactions with others.[94]

This concatenation of data is immensely valuable to advertisers and has proven an irresistible temptation to government.[95] One harm stemming from toxic data is that citizens' speech may be chilled due to this hybrid corporate-government dragnet surveillance.[96] Even after the reforms of the USA Freedom Act,[97] call data from most telephone calls in the United States is gathered by carriers and stored for access by the National Security Agency (NSA) under rolling orders from the Foreign Intelligence Surveillance Court (FISC).[98] Under current law, nothing prevents Internet service providers (ISPs), mobile manufacturers, and the NSA from doing the same with web-traffic or geolocation data (although now the NSA might now not hold some data directly).[99] The NSA denies such surveillance of web queries and geolocation information, but recent revelations demonstrate that it has the technology, has used or experimented with such programs in the past, and has the go-ahead from the FISC,

94. *See* G.S. Hans, *Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for A New Era*, 19 MICH. TELECOMM. & TECH. L. REV. 163, 164 (2012) (describing the routine collection and sale of user data collected by various websites).

95. *See id.* (describing the broad market for Internet user data among advertisers and other third parties); Richards, *supra* note 14, at 1958 ("One of the most significant changes that the age of surveillance has brought about is the increasing difficulty of separating surveillance by governments from that of commercial entities. Public- and private-sector surveillance are intertwined . . . [as] their digital fruits can easily cross the public/private divide.").

96. *See* Scott Michelman, *Who Can Sue over Government Surveillance?*, 57 UCLA L. REV. 71, 78 (2009) ("People who believe that they are being surveilled might avoid . . . expressing opinions that could subject them to further investigation.").

97. *See* USA Freedom Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (restoring in modified form several provisions of the Patriot Act, the Freedom Act imposes new limits on the bulk collection of telecommunication metadata on U.S. citizens by American intelligence agencies, including the National Security Agency).

98. *See* Timothy B. Lee, *Everything You Need to Know About the NSA's Phone Records Scandal*, WASH. POST: WONKBLOG (June 6, 2013), http://www.washingtonpost.com/news/wonkblog/wp/2013/06/06/everything-you-need-to-know-about-the-nsa-scandal [http://perma.cc/7G3J-RQUJ] ("[T]he NSA is seeking [phone] records from everyone, even if they've never made an international phone call.").

99. *See* Emma Roller, *This Is What Section 215 of the Patriot Act Does*, SLATE: WEIGEL (June 7, 2013), http://www.slate.com/blogs/weigel/2013/06/07/nsa_prism_scandal_what_patriot_act_section_215_does.html [http://perma.cc/Q8QM-EBJW] (explaining that the NSA's data collection is authorized under Section 215 of the Patriot Act, and that the Section appears to "appl[y] not only to phone metadata but also to email, chats, photos, video, logins, and other online user data").

although the Second Circuit's decision in *ACLU v. Clapper*[100] may give it pause as to the legality of this approach.[101]

Aggregated data contributions serve to train machine learning algorithms, such that the data offered by one person trains an algorithm that impacts someone else.[102] For example, Future Attribute Screening Technology (FAST) is a crime-prediction program developed by the Department of Homeland Security. The purpose of the program is to "rapidly identify suspicious behavior indicators to provide real-time decision support to security and law enforcement personnel."[103] The program focuses on identifying "malintent," the present intent to commit future bad acts.[104] Volunteers are asked to perform disruptive acts, so that a machine learning algorithm may study baseline data of malintent to associate with behavioral indicators. The system focuses on a wide range of factors, such as heart rate, body movement, movement of the eyes, or pupil dilation, which might give away someone who is thinking of committing a disruptive act. The volunteers' donation of information about themselves teaches the algorithms about others and, when the program is active, may result in the arrest and detention of people

100. ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015).

101. *See* Charlie Savage, *In Test Project, NSA Tracked Cellphone Locations*, N.Y. TIMES, Oct. 3, 2013, at A13 (suggesting that "any long-term, automated collection of a person's publicly displayed actions might raise Fourth Amendment issues"); *see also* Gregory Ferenstein, *NSA Uses Facebook and GPS Data to Identify Suspects in Networks of Americans*, TECHCRUNCH (Sept. 28, 2013), http://techcrunch.com/2013/09/28/nsa-uses-facebook-and-gps-data-to-identify-suspects-in-networks-of-americans [http://perma.cc/R7HA-LWSB] (describing a comprehensive GPS tracking program ostensibly targeted at non-U.S. persons); Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'*, THE GUARDIAN (July 31, 2013, 8:56 AM), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data [http://perma.cc/CT6Y-N3N9] (stating that "NSA analysts have exceeded even legal limits as interpreted by the NSA in domestic surveillance"). For the legal underpinnings of these metadata-collection programs, see *In re* FBI for an Order Requiring the Production of Tangible Things from [*redacted*], No. BR 13-109, 2013 WL 5741573, at *1 (FISA Ct. Aug. 29, 2013); Opinion and Order, [*redacted*], No. PR/TT [*redacted*] (FISA Ct. [*redacted*]), http://dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf [http://perma.cc/HTX7-GXGH]. *But see Clapper*, 785 F.3d at 826 (reversing and remanding the district court's determination that Section 215 of the Patriot Act authorized bulk telephony-metadata collection by the NSA).

102. *See* MacCarthy, *supra* note 1, at 445 ("Privacy externalities are composite. . . . The first step in understanding negative privacy externalities is to understand how data collectors, aggregators, and analysts can infer information about individuals . . . .").

103. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST) PROJECT 2 (2008), https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf [https://perma.cc/D3E4-6PNC].

104. *See id.*

based on their supposed malintent.[105] That is, the generosity of volunteers with respect to their personal data creates a system that almost exclusively impacts others.

C. Privacy's Individualism Bias

While the reality of data sharing and parsing has changed, privacy theory has lagged. Privacy theorists differ famously and widely on the proper conception of privacy,[106] but these many theories tend to share an underlying theoretical assumption. Most dominant theories of privacy view it through the lens of individualism.[107] These theories may touch on the social dimension of privacy,[108] but they do not strongly engage the social dilemma of privacy.[109]

1. *Individualism's Historical Influence*. To show the deep roots of individualism's hold on privacy discourse, we draw on foundational examples.[110] Consider *The Right to Privacy*,[111] the seminal U.S. work on legal protection of privacy by attorney Samuel Warren and future

---

105. *See generally* Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. (forthcoming Sept. 2015) (arguing that the government's overreliance on big data and metadata may deprive citizens of their due process rights).

106. *See* Solove, *Privacy*, *supra* note 64, at 1099–1123 (gathering and challenging essentialist conceptions of privacy).

107. *See* REGAN, *supra* note 38, at 3; Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 958 (1989) ("[P]rivacy rests upon an individualist concept of society.").

108. *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1664 (1999) [hereinafter Schwartz, *Privacy and Democracy*] ("As Post observes, information privacy is not 'a value asserted by individuals against the demands of a curious and intrusive society,' but a necessary aspect of relations with others."); *see also* Post, *supra* note 107, at 962–63 (noting that "each 'individual must rely on others to complete the picture of him of which he himself is allowed to paint only certain parts'").

109. We are not the first to note the zeroing in on individualism. As Priscilla Regan writes, "[I]n policy debates in the United States, the emphasis has been on achieving the goal of protecting the privacy of individuals rather than curtailing the surveillance activities of organizations. . . . It was thought that by protecting individual privacy, the surveillance activities of organizations and the government would be checked." REGAN, *supra* note 38, at 3. Thus, "[a]lthough privacy is viewed as a boundary separating the individual from society, the dominant assumption has been that only the individual has an interest in that boundary." *Id.* at 23. The result has been an emphasis on an atomistic individual and the legal protection of his or her rights. *Id.* at 214. The results have not been positive for privacy theory: "[I]ndividualistic conception of privacy does not provide a fruitful basis for the formulation of policy to protect privacy." *Id.* at 4.

110. For a more extensive treatment of the history of individualism in privacy theory, see *id.* at 24–41.

111. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

Justice Louis Brandeis. The article explores the relationship between changing social mores and developing technology. Warren and Brandeis discuss the increased intrusiveness of technology and the media. Photography and newspapers served as the catalyst for the crystallization of privacy rights out of the common law. Warren and Brandeis's approach has proven both technologically and legally prescient. For example, they wrote that "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[112] The same could have been written about Twitter, Facebook, Instagram, or Snapchat.

Yet even Warren and Brandeis's visionary approach relied on private rights defended by individuals. Warren and Brandeis' "right to be let alone" is an individual right, not a tool that helps groups navigate a social dilemma. For example, they wrote that "[r]ecent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right 'to be let alone.'"[113] They considered their "purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is."[114] Once noted, the focus on individualism is found throughout: "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others,"[115] they noted, concluding that "[i]n every such case the individual is entitled to decide whether that which is his shall be given to the public. No other has the right to publish his productions in any form, without his consent."[116]

The traditional right to privacy as formatively expressed by Warren and Brandeis contemplates an individual's control of information that originates from or bears on that individual and is therefore hers exclusively to reveal or protect. It does not focus on the spillover effects of information that is not just about me, or you, but us. The traditional approach does not focus on group

112. *Id.* at 195.
113. *Id*.
114. *Id*. at 197.
115. *Id.* at 198.
116. *Id.* at 199.

coordination as the problem, or on known solutions to the social dilemma. Overlaps exist, of course. Perhaps were Warren and Brandeis to write today, they might pen a new *Right to Privacy*, which would note that person A's disclosure of seemingly innocuous information could be aggregated by computers, stored in functionally infinite databases, and then used to train machine learning algorithms that may negatively affect B and everyone else. But to do so requires a further development of the theoretical underpinnings of privacy to shed light on how certain information is not the individual's private and exclusive domain, but rather bears on everyone.

2. *Individualism in Modern Notice and Choice.* Modern privacy approaches have developed and intensified the emphasis on individual notice, choice, and control over information flows.[117] For example, privacy as control has emerged as a dominant theory of informational privacy,[118] in part because it promises individuals (rightly or wrongly) the ability to both disclose and control dissemination of information online.[119]

Although privacy as control is not an incurably individual-centered approach because the tools of control could be handed to groups,[120] the theory's subsequent development and, above all, its operationalizing regime of notice and choice demonstrate the

117. *See* REGAN, *supra* note 38, at 24–41 (tracing the post–*Right to Privacy* history of overemphasis on individualism through legal and philosophical thought).

118. *See* THOMAS NAGEL, CONCEALMENT AND EXPOSURE 4 (2002); JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 5 (2000); ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) (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"); Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) ("Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves."); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1167 (2004) ("The idea that privacy is really about the control of one's public image has long appealed to the most philosophically sophisticated American commentators, from Alan Westin, to Charles Fried, to Jeffrey Rosen, to Thomas Nagel.") (citations omitted); *see also* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 820 (2000) [hereinafter Schwartz, *Internet Privacy*] ("The weight of the consensus about the centrality of privacy-control is staggering.").

119. *See* MacCarthy, *supra* note 1, at 434 ("The informed consent model is entirely focused on the individual.").

120. *See* WESTIN, *supra* note 118, at 7 ("[P]rivacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.").

dominance of individualism in modern privacy law.[121] Notice and choice depend entirely and explicitly on individuals. Such regimes attempt to ensure that individuals know what is being done with their information, and have some choice as to how or whether that data is used. Notice is provided to the individual about information pertaining to the individual, and the choice is the individual's to make.

Even critiques of notice and choice tend to buy into the individual paradigm, rather than challenging the baseline assumption of individuality. The traditional response to the flaws of notice-and-choice regimes has been that the notice and choice are not yet robust enough.[122] The standard criticism is that consumers are not sufficiently informed about what is being done with their information, and they have not been given enough discretion in controlling their privacy. A standard solution is to argue that the quality of the notice and choice must improve. To achieve this, terms of use and end-user license agreements are made ever-more explicit at the direction of courts and regulators. The focus on comprehension and control supposedly enables the consumer to understand the consequences of her revelation of information about herself and control the information she offers about herself.[123] In turn, the privacy-by-design regulatory trend is intended to incentivize companies to build tools that empower individual understanding and control.[124]

This is not to say that notice and choice are not useful, merely that individual-focused education and empowerment appear to yield diminishing returns.[125] Consumers quite rationally do not read the

121. *See* REGAN, *supra* note 38, at 27 ("[I]n two important areas Westin's analysis moves away from further development of that social importance of privacy: the first involves his discussion of the importance of privacy to the individual and the second his analysis of the balance between privacy and other interests.").

122. *See, e.g.*, Jeff Sovern, *Opting in, Opting out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1094 (1999) (noting that consumers are not currently well informed and "often find it difficult to opt out").

123. *See* Bamberger & Mulligan, *supra* note 32, at 301–02 ("Thus, the appropriate privacy-protective behavior entails 'mak[ing] secondary uses of information only with clear, unequivocal user consent and control, and test[ing] these controls to ensure that the default settings match with the expectations of the user.'").

124. ANN CAVOUKIAN, INFO. & PRIVACY COMM'R OF ONTARIO, PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES 1–2 (Jan. 2011), http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf [http://perma.cc/WY97-SSAA].

125. *See* Solove, *Introduction*, *supra* note 61, at 1881 ("[E]ven well-informed and rational individuals cannot appropriately self-manage their privacy due to several structural problems.").

carefully redrafted privacy policies.[126] Even if they did, the controls produced by companies in response to privacy-by-design incentives are often left unused because of time costs of vigilance or complexity.[127] Privacy by design has delivered strong back-end protection for consumers' personal information that corporations deem proprietary, but it has not delivered strong front-end protection for information as consumers disclose it.[128]

Even if individualized notice and choice did function as desired—and it does not—there would still be a problem. The notice-and-choice approach to privacy assumes incorrectly that the individual is the predominant unit in the privacy conversation, and thus that each individual can and should manage information solely about herself.[129] This is an oversight.[130] By consenting to information gathering, a user becomes a conduit for gathering information about her entire social network, whether or not they have consented.[131]

---

126. *See* Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard-Form Contracts*, 43 J. LEGAL STUD. 1, 2 (2014); Florencia Marotta-Wurgler, *Does Contract Disclosure Matter?*, 168 J. INSTITUTIONAL & THEORETICAL ECON. 94, 94 (2012); Florencia Marotta-Wurgler, *Does Increased Disclosure Help? Evaluating the Recommendations of the ALI's 'Principles of the Law of Software Contracts'*, 78 U. CHI. L. REV. 165, 173 (2011); Solove, *Introduction*, *supra* note 61, at 1884 ("Most people do not read privacy notices on a regular basis."); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 667 (2014) ("Social science research reveals that consumers do not read or understand privacy policies, are heavily influenced by the way choices are framed, and harbor many preexisting assumptions that are incorrect. . . . [A]ccording to one study . . . 75% falsely believe that when 'a website has a privacy policy, it means the site will not share my information with other websites and companies.'").

127. *See* Emil Protalinski, *Survey: Facebook, Google Privacy Policies Are Incomprehensible*, ZDNET (May 4, 2012), http://www.zdnet.com/blog/facebook/survey-facebook-google-privacy-policies-are-incomprehensible/12420 [http://perma.cc/G542-FF8F] (discussing the fact that "consumers [have] a very poor understanding of how Facebook and Google track and store user information").

128. *See* Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 418 (2013) (noting the failure of current online privacy solutions to "tackle the 'front-end' of [the problem]").

129. *See, e.g.*, Bamberger & Mulligan, *supra* note 32, at 247 ("Scholars and advocates criticize [U.S. privacy policy] as weak, incomplete, and confusing, and argue that it fails to empower individuals to control the use of their personal information.").

130. *See* MacCarthy, *supra* note 1, at 444 ("I want to draw attention to and emphasize another way in which informed consent does not legitimize the use of information. These are contexts that exhibit substantial privacy externalities.").

131. *See* Michal Kosinski, David Stillwell & Thore Graepel, *Private Traits and Attributes are Predictable from Digital Records of Human Behavior*, 110 PROC. NAT'L ACAD. SCI. U.S. 5802, 5802–05 (2013) (describing their study in which users' personal attributes were predicted with high rates of accuracy based on their Facebook likes); Solove, *Privacy*, *supra* note 64, at 1104

Even if regulators were to succeed in making individualized consent to data gathering meaningful, the intervention would miss the essential point. Educated and empowered consumers would still have little say, because even if perfectly informed and empowered, they only control their own data, and cannot influence the sea of information from which big data algorithms work.[132] The old canard that if an individual does not like a social network, she need not use it misses a critical point.[133] Because so much information is provided by third parties, no one can truly opt out.[134] If a person is not on the network herself, she can opt out of its individual benefit, but still bear (most of) its individual cost.

The very notion of individual control or individual-centered notice and choice complicates group efforts to maintain coordination in the face of a social dilemma. To demonstrate the problem, we offer a thought experiment, which we term the "informed prisoner's dilemma." Consider a standard prisoner's dilemma. If both prisoners stay mum, they both get a mild punishment of one year in jail. If both prisoners sell each other out, they each get five years. If one prisoner stays quiet while the other squeals, then the one who stays quiet gets ten years in prison, and the rat gets none. Individually, each prisoner will always want to squeal.[135] No matter what the other prisoner does, a prisoner who squeals is better off. But the socially maximized outcome (for the prisoners, of course) is for them to cooperate. If we

("[P]ersonal information rarely belongs to just one individual; it is often formed in relationships with others."); Jennifer Golbeck, *Smart People Prefer Curly Fries*, SLATE (Oct. 7, 2014, 7:48 AM), http://www.slate.com/articles/technology/future_tense/2014/10/youarewhatyoulike_find_out_what_algorithms_can_tell_about_you_based_on_your.html [http://perma.cc/9VSZ-SD7W] ("[T]he most important lesson to take away from these algorithms is that you cannot control what is predicted.").

132. *But see* MacCarthy, *supra* note 1, at 446 ("An information externality occurs when one person's revelation of information reveals something about someone else.").

133. *See* Solove, *Introduction*, *supra* note 61, at 1881 ("Privacy . . . fosters a certain kind of society, since people's decisions about their own privacy affect society, not just themselves. Because individual decisions to consent to data collection, use, or disclosure might not collectively yield the most desirable social outcome, privacy self-management often fails to address these larger social values.").

134. For example, Facebook maintains a "shadow social network" of information about users who do not use Facebook—populated by information provided by users who do. Violet Blue, *Firm: Facebook 'Bug' Worse Than Reported; Non-Users Affected Too*, ZDNET (June 26, 2013, 6:05 PM), http://www.zdnet.com/firm-facebook-bug-worse-than-reported-non-users-also-affected-7000017318 [http://perma.cc/ARF2-M8K6].

135. *See, e.g.*, Kreps et al., *supra* note 48, at 246 (explaining how the Nash Equilibrium path of a prisoner's dilemma game results in an incentive structure in which each prisoner will always want to defect).

consider the prisoners as a group, then cooperating prisoners will suffer only two years' worth of penalty instead of the ten that they collectively would suffer if either or both squeal. Neoclassical economics therefore predicts that both parties will reach the socially suboptimal decision to squeal.

Yet conceivably the prisoners, being experienced at this sort of thing, may at first choose not to rat one another out. One way to stop this welfare-maximizing cooperation is to inform and empower the individual participants as to the nature and likely outcomes of the social dilemma. Imagine taking one prisoner out of the room, sitting her down, and informing her at great length about the nature of the dilemma, including the fact that she is better off defecting no matter what the other prisoner does. Consider the effect of empowering the prisoner's decision, so that she is certain her decision to defect will be honored and will with certainty have the described effect. Providing the ordinary prisoner with that mental model might change how she sees the situation and might, thereby, make the dilemma worse. In short, if privacy is a social dilemma, the very education and empowerment that regulators rely on to ameliorate the dilemma may instead exacerbate it.

3. *Individualism in the Transatlantic Privacy Discourse.* The individualism bias also crosses major cultural and legal divides in privacy law. For example, approaches to privacy appear at first blush to play out differently on each side of the Atlantic.[136] One narrative is that the United States focuses on liberty,[137] while the European Union focuses on human dignity.[138] Yet both philosophies look at privacy as a matter best resolved by informing and empowering individuals.[139] In both Europe and the United States, the presumed goal is for fully

136. *See* Whitman, *supra* note 118, at 1160 (explaining how the United States and Europe do not possess "general 'human' intuitions about the 'horror of privacy violations,' but instead have different institutions that shape privacy protection norms").

137. *See id.* at 1158 (arguing that the American notion of "privacy" is strongly connected to the idea of "liberty" by example of constitutional-rights cases argued on basis of the right to privacy).

138. *Id.* at 1161 ("Continental privacy protections are, at their core, a form of protection of a right to *respect* and *personal dignity*.").

139. As a matter of private law, the functional difference is in the ability to consent to corporate data gathering. In Europe, and speaking extremely broadly, consent to corporate data tracking is opt-in. In the United States, consent is opt-out. *See* Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 281, 287 (2012).

informed individuals to consent to the use of their individual data. The problem remains: the data does not impact that individual alone.

The Atlantic divide in privacy theory therefore cloaks an underlying similarity.[140] In both legal orders, individuals consent to the use of data that impacts nonconsenting third parties.[141] Both the liberty and dignity approaches focus on empowering and informing individuals, rather than improving group coordination.[142] U.S. and European law differ on whether individuals must opt in or opt out of data collection and processing. They differ on the scope and timing of the individual's consent. They differ on the powers an individual may wield—whether an individual may demand that Google delete stale information pertaining to her, for instance.[143] But both traditions locate the problem and its solution with the individual deciding in isolation—the individual must opt in or opt out.[144] The individual must consent to out-of-context uses. The individual must pursue deletion of data that pertains to her. In both the United States and Europe, the law provides tools to help individuals understand and control information that directly concerns them. Both traditions lack tools that help groups of individuals manage coordination problems. And both traditions have little to no protection for spillover effects of information—information about person A that nevertheless imposes negative effects on person B, and everyone else.[145]

The above discussion attempts to point out the serious bias in favor of conceptualizing privacy in terms of individual information, rights, and actions. This bias was present in the foundational conceptions of a legal right to privacy, and lives on today as an

---

140. *See* Whitman, *supra* note 118, at 1163 (explaining how the differences between the two theories are *relative*, but not *absolute*).

141. *See* Tene & Polonetsky, *supra* note 139, at 285 (analogizing that placing the burden of consent on users is "tantamount to imposing the burden of healthcare decisions on patients instead of doctors," due to the complexity of the online-information ecosystem).

142. *See* Whitman, *supra* note 118, at 1167–68 (explaining how the European conception of privacy, the "right to a *public* image of our own making," comes from the same root as its American counterpart, "the right to control our public face").

143. *See, e.g.*, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN [http://perma.cc/ED5L-DZRK] (holding that Google must delete stale personal data).

144. *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, 260–62 (2013) (arguing that "[t]he consent model is flawed from an economic perspective").

145. *See* Lau, *supra* note 62, at 266 ("If a citizen wishes to be left alone on the Internet, and takes no steps to be on the Internet, the law does not provide any meaningful remedy for when a third party publishes information about that citizen on the Internet.").

underlying assumption in the modern operationalization of privacy as control through notice-and-choice regimes. Further, a comparison of the U.S. and E.U. approaches shows that for all their differences, approaches to privacy in the United States and Europe both focus on individualism—one philosophy is informed by individual dignity, and the other by individual liberty. As a result, the social dilemma of privacy has gone underexamined in legal theory, as the following Subpart will discuss.

D. Conceptions of the Public Good in Privacy Theory

We discuss here three broad types of legal analysis of the social dimension of privacy. First, theorists often address the social dimension of privacy by generalizing from the individual case.[146] For example, Alan Westin described privacy as the individual withdrawal from society.[147] Under this approach, social privacy is valued primarily because it guarantees individual privacy.[148] Social welfare is a fortuitous byproduct of happy individuals. A second set of analyses treats privacy as a threat to the public good, usually defined as some sort of interest in preserving security against criminals or terrorists.[149] Finally, there is a nascent literature touching on privacy as a public good, often through the lens of environmental regulation.[150] We touch on each in turn. We note in conclusion that there is no treatment of privacy as a public good that examines the public-goods literature for tools to empower groups to resist privacy's social dilemma.

1. *Privacy in the Public Good*. The first grouping of legal analysis asserts that privacy is in "the public good." This can be difficult to distinguish from claims that privacy is "a public good." These terms belong to different disciplines. When a lawyer discusses "the public good," and an economist explores "a public good," they are likely talking about two quite different things. *The* public good refers to what is good for the public. *A* public good refers to a good, a product, which is produced by groups under certain conditions that

146. *See, e.g.*, REGAN, *supra* note 38, at 27–28 (discussing Alan Westin's turn from social to individual accounts of the value of privacy, and offering a critique of the resulting overindividualization of Westin's theories).

147. *See id.* at 28.

148. *See id.*; *see also infra* Part I.D.1.

149. *See infra* Part I.D.2.

150. *See infra* Part I.D.3.

create a tension between selfishness and cooperation.[151] *The* public good is a general assertion that the public will be better off if x or y state is the case. *A* public good is a product, good, service, or other benefit that may not be produced, because everyone can share equally in it, whether they contribute to it or not. *The* public good does not necessarily suffer from a free-rider problem. *A* public good is defined by a free-rider problem.[152] Actions taken to promote *the* public good are not necessarily social dilemmas. *A* public good necessarily involves a social dilemma.[153] If one defines *the* public good as welfare, normally *the* public good increases if *a* public good is provided. Yet welfare is a broader concept, and one need not define *the* public good in terms of welfare theory. But it is also quite clear that not everything that is in *the* public good is necessarily *a* public good.[154]

Much legal scholarship begins with the premise that individual privacy is good, and that because it is good, protecting privacy is socially beneficial, or in the public good.[155] The problem is that the similarity in surface terminology, combined with the vague use of economic language, means that many legal analyses are confusing as to whether they truly address a public good. An assertion that privacy is a public good may mean simply that the author believes privacy is good, and will benefit the public.[156] The assertion that something is good for each citizen individually does not mean that it is good for

---

151. *See* Ledyard, *supra* note 10, at 111–13.

152. *See id.* at 112 ("There are many theories [regarding what happens in public goods experiments]. One, the economic/game-theoretic prediction, is that no one will ever contribute anything. Each potential contributor will try to 'free ride' on the others.").

153. *See id.* (explaining that "the group would be best off . . . (taking home $10 each) if all contributed $5. . . . From the point of view of this theory, individual self-interest is at odds with group interest").

154. Actually, "*a* public good" can well be at variance with "*the* public good." The classic illustration is a cartel. For each cartel member, it is individually best if all other cartel members sell at a high price, while she undercuts and attracts all trade. Hence from the perspective of the cartel members, cartel discipline is a public good. Yet antitrust authorities intervene whenever they spot a cartel because, for the demand side of the market, and for welfare, price fixing is undesirable.

155. *See* REGAN, *supra* note 38, at 27–29 (surveying the literature).

156. *See, e.g.*, Joshua S. Levy, *Towards a Brighter Fourth Amendment: Privacy and Technological Change*, 16 VA. J.L. & TECH. 502, 511 (2011) ("[U]nlike the rights of an individual criminal suspect, [privacy] is a public good."). Levy does define public goods carefully, and it is clear he is on the right track, but his distinction does not stand: the individual rights of defendants ought to be, to his analysis, the same good as privacy because it benefits us all when criminal defendants have rights. This public good is different from a true public good, a common good to which all share undivided nonexclusive access.

society as a whole—that is precisely the nature of a social dilemma. So assertions that privacy is an individual right which, when enjoyed by society as a whole, is beneficial, do not capture the tension at the heart of public goods.

2. *Privacy Against the Public Good*. Especially in political discourse, privacy is sometimes portrayed as standing in tension with the public's interest in security, that is, that privacy is against the public good.[157] The argument is simple and seductive. Bad people desire privacy to hide their bad acts. What a criminal seeks to keep private, the public wants to know. Thus, as Judge Richard Posner noted, "[m]uch of what passes for the name of privacy is really just trying to conceal the disreputable parts of your conduct . . . . Privacy is mainly about trying to improve your social and business opportunities by concealing the sorts of bad activities that would cause other people not to want to deal with you."[158] To this way of thinking, privacy interests stand in tension with community interests, and must therefore be curtailed in the name of the public good. This tension between individual privacy and public need to know particularly influences modern discussions of the reach and role of the surveillance state.[159] We address this approach because it asserts a relationship between privacy and the public good, albeit one with which we and others strongly disagree.[160]

The argument starts from a false point of departure, assigning negative value to all information that anyone may wish to keep

157. *See* Louis Henkin, *Privacy and Autonomy*, 74 COLUM. L. REV. 1410, 1410 (1974) ("Governments . . . frequently confront 'private rights' with the 'public good,' implying tension between them that requires choice or accommodation.").

158. Grant Goss, *Judge: Give NSA Unlimited Access to Digital Data*, PC WORLD (Dec. 4, 2014, 1:46 PM), http://www.pcworld.com/article/2855776/judge-give-nsa-unlimited-access-to-digital-data.html [http://perma.cc/649V-9WTR]; *see also* Richard Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 394–401 (1978) (explaining the concept of information concealment in greater depth).

159. *See, e.g.*, Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262, 272 (2013) ("[A]ny account of surveillance's privacy harms is often resisted on the grounds that some surveillance is essential for the public good. But there is a line between surveillance that is essential for the public good and invasive total-information awareness technologies, and that line is easy to cross if unattended.").

160. *See, e.g.*, Scott E. Sundby, *"Everyman's" Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1809 (1994) ("The pressing needs of an immediate crisis almost always will seem to justify a government intrusion . . . . Looked at in isolation, it is better to have the shoreline of one's island of privacy partially eroded by government surveillance than to have the entire island overrun by barbarians.").

private. Thus, for example, Posner does not wish a person to hide from a future potential spouse that he is sterile.[161] By selecting harmful characteristics, Posner tautologically ensures that hiding the characteristic will cause harm. But this dynamic does not hold for the vast majority of private information. It is certainly untrue of democratic activists in totalitarian countries, people with high potentiality but no certainty of rare genetic disorders, persecuted religious or racial minorities, individuals with a minority sexual orientation, or with any of a raft of other traits. Keeping those traits hidden has no possible bearing on the economic decisions Posner supports, except that counterparties or the government may misuse the information. Posner suggests rationality will trump prejudice,[162] but numerous examples, from employment discrimination to religious persecution, put paid to that notion. Even more important: Ex-post comparison of the benefit (for a third party) and the harm (for the person whose private information is at stake) misses the point. The normatively appropriate comparison is ex ante. It must balance *all* benefits and *all* harms from making the piece of information in question accessible.

In its most recent security-focused incarnation, the argument that privacy cuts against the public good falls short because it both creates a false dichotomy between privacy and security, and does not adequately account for harms created by mass surveillance.[163] Treating privacy as a security threat trades fear of terrorists for fear of one's own government. Or, to cast things in the language of public goods, security is likely also a public good, with its own production function and its own problems of free riders or exploiters. But that does not settle the role of privacy within that production function. The question is whether one treats privacy-seeking behavior as creating an entirely private benefit outweighed by the social costs it creates for the group, or whether one treats privacy as part of the stock of social welfare, such that reducing privacy reduces social

161. *See* Posner, *supra* note 158, at 399 ("Other private information that people wish to conceal, while not strictly discreditable, would if revealed correct misapprehensions that the individual is trying to exploit, as when a worker conceals a serious health problem from his employer or a prospective husband conceals his sterility from his fiancée.").

162. *See* Posner, *supra* note 11, at 406.

163. *See generally* DANIEL SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011) (arguing that many security-based arguments posit a false trade-off between privacy and security, and that surveillance imposes serious costs even on those who believe they have nothing to hide and therefore nothing to fear from surveillance).

welfare. We view a secure private life as an integral part of security, not a threat to it.

Separately, there may well be opportunity costs between public goods, but it is not our aim to settle the debate as to which projects the public should choose. Nor is it useful to pit public goods against one another in pairwise comparisons. Why should we pit security versus privacy, and not against public education, or clean air, or any of millions of other public goods, or against the sum of all of those? We admit that there are myriad different public goods. The existence of many public goods does not reduce the need to examine each, and to maximize social welfare from investment in that good. Thus, while there may be opportunity costs between public goods in general, and even between security and privacy in particular, we maintain that exploring how to maximize the social value of privacy is valuable regardless of any trade-off effects between privacy and security.

3. *Toward Privacy as a Public Good*. The legal literature is not entirely devoid of the suggestion that privacy can be profitably studied as a true public good.[164] For example, Paul Schwartz notes that "information privacy functions as a type of public good, like clean air or national defense"[165] and that "[p]rivacy, from a constitutive perspective, is also a 'public good.' Information privacy is a kind of commons that requires some degree of social control to construct and then preserve."[166] Priscilla Regan discusses the "collective value" of privacy, which she "derive[s] from the economists' concept of collective or public goods."[167] Regan suggests that "[r]ecognition that privacy has some features of a public or collective good would make clearer the institutional or organizational interests in personal information and the weaknesses of a market solution in providing

164. *See, e.g.*, Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1253–54 (2002); Schwartz, *Internet Privacy*, *supra* note 118, at 832–33; Schwartz, *Privacy and Democracy*, *supra* note 108, at 1698; Schwartz, *Property*, *supra* note 30, at 2084–85 ("[I]nformation privacy functions as a type of public good, like clean air or national defense."); Paul M. Schwartz, *Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technology*, 53 WM. & MARY L. REV. 351, 367–68 (2011).

165. Schwartz, *Property*, *supra* note 30, at 2084–85.

166. Janger & Schwartz, *supra* note 164, at 1253–54.

167. REGAN, *supra* note 38, at 227.

privacy protection."[168] We take this suggestion as an invitation for a full analysis of privacy in light of what the public-goods literature of the past several decades has learned.[169]

We further note a nascent literature that draws on existing environmental regulatory approaches to propose solutions to the problem of toxic data.[170] The eco-privacy literature shares a base set of concerns with our public-goods analysis. For example, Dennis Hirsch analogizes spam to pollution,[171] suggesting that privacy (in this sense, freedom from spam) is subject to a tragedy of the commons.[172] Michael Froomkin uses a similar characterization: "Many mass data-collection activities, particularly those that take place in or through public spaces can be usefully analogized to pollution of the private sphere."[173] Eben Moglen notes that "[surveillance] is not the first, the last, or the most serious of the various forms of environmental crisis brought on in the last two centuries by industrial overreaching."[174] There are therefore some similarities between our approach and the framing language of the environmental-privacy literature.[175] That literature has the particular advantage of drawing on a rich and successful regulatory tradition, which has ironed some of the kinks out of helping industrial communities find and implement low-cost, high-value changes. As such, it provides a strong set of analogies for

168. *See id.* at 231; *see also* MacCarthy, *supra* note 1, at 447 ("When privacy is thought about as involving an externality, it is inherently social because privacy decisions made by some actors inevitably affect the economic interests of others.").

169. *See* Schwartz, *Property*, *supra* note 30, at 2076 ("This Part examines and re-evaluates the skepticism regarding property rights in personal data; the following Part develops a model for propertization of personal data that accommodates these concerns."); *see also id*. at 2085 ("The traditional problem with relying on a property regime to supply a public good follows from two of the good's qualities—nonrivalrous consumption and nonexcludability. A privacy commons illustrates both of these aspects of public goods.").

170. *See* A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 ILL. L. REV. 1713; Hirsch, *Inner Environment*, *supra* note 26, at 10; Dennis D. Hirsch, *The Glass House Effect: Big Data, the New Oil, and the Power of Analogy*, 66 MAINE L. REV. 374, 375 (2014) [hereinafter Hirsch, *Glass House Effect*]; Moglen, *supra* note 92.

171. Hirsch, *Inner Environment*, *supra* note 26, at 15–18.

172. *Id*. at 24–28.

173. Froomkin, *supra* note 170 (manuscript at 30).

174. Moglen, *supra* note 92.

175. *See* Hirsch, *Glass House Effect*, *supra* note 170 ("If data is the new oil, then these data releases are the new oil spills."); *see also* Hirsch, *Inner Environment*, *supra* note 26, at 28 ("When a web site gathers and sells personal information about one of its users, . . . they cause that individual to lose a degree of privacy. This cost is borne by the user and is external to the business. It is a negative externality.").

how to craft and maintain political coalitions to resolve particularly harmful collective-action problems.

Yet our approach involves some important differences. Whereas the environmental-privacy literature draws on environmental law and the history of environmental regulation for inspiration, we draw on public-goods models and experiments, and hence focus on the behavioral dimension of the question. Environmental law is chiefly shaped by the experience of government in seeking to rein in large-scale polluters.[176] As a result, the environmental-privacy literature suggests government action or legislation to resolve the collective-action problem of privacy.[177] Whereas the example of environmental law suggests regulation to resolve collective-action problems, we suggest group tools to sustain cooperation with minimal outside intervention.

The eco-privacy literature brings a fresh and welcome perspective, as well as a history of experience with practical implementation, especially for regulating high-volume polluters. Not all collective-action problems are the same, however. In considering that privacy may be a public good, we focus less on large-scale offenders who are most analogous to the factories of environmental-law analysis, and more on the small but constant contributions that users make exposing data about one another, the prisoners in a prisoners' dilemma. Both approaches are needed. Broad privacy legislation may be necessary to restrain mass consumer surveillance, and environmental law may offer a good place to start. On the other hand, broad privacy legislation has proven hard to pass, despite the broad base of popularity among the electorate for enhanced privacy. Whether or not such efforts succeed in the current political climate, another path remains open.

This is where our approach parts ways (amicably) with the environmental-privacy literature. Instead of following a Pigouvian approach of seeking government intervention to tax or sanction bad

176. *See* Hirsch, *Inner Environment*, *supra* note 26, at 4 (comparing the information revolution to the Industrial Revolution, which "generated an unprecedented level of environmental degradation that far outstripped the ability of the existing legal system to deal with it").

177. *See id*. at 43 (proposing a cost per spam email that would render spam activity unprofitable); *see also* Froomkin, *supra* note 170 (manuscript at 30) (proposing the use of Privacy Impact Notices "before allowing large public or private projects which risk having a significant impact on [privacy]").

institutional behavior,[178] we follow in the tradition of Coase and Ostrom,[179] and mine the economics literature for tools groups themselves can use to sustain production of public goods, or in this case to maintain privacy. We are inspired less by environmental law, and more by the results of public-goods experiments. 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.

II. PRIVACY AS A PUBLIC GOOD

This Part draws on the past several decades' worth of advances in public-goods theory and experiments. The Part then highlights certain specific group institutions, which appear repeatedly in this literature, as being particularly worthy of consideration for building tools to help groups resist the social dilemma of privacy.

A. Public Goods and Bads

Since public goods are desirable as a matter of definition, and public bads are undesirable on a like definition, the question is why there are too few public goods and too many public bads. The difficulty lies in the interface between society and individual. If a public good must be produced in order for it to exist, then the radically nonrival nature of the good becomes a barrier to its production.[180] Since each individual shares in the good equally if produced, individuals have no incentive to contribute to the costs of producing the public good.[181] Because such free riders benefit from

178. *See* CORNES & SANDLER, *supra* note 3, at 16 ("Governments were viewed as outside agents who, through the imposition of taxes (or subsidies), could induce the externality generator to limit (or increase) his or her activity so as to achieve efficiency.").

179. DRAMA, *supra* note 31; Ronald Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 42–44 (1960).

180. Guido Pincione, *Market Rights and the Rule of Law: The Case for Procedural Constitutionalism*, 26 HARV. J.L. & PUB. POL'Y 397, 414–15 (2003) ("Nobody has an incentive to contribute to the production of a public good, since anybody can take a free ride on others' productive efforts.").

181. *See id*. Technically, the prediction that the good will not be provided at all hinges on the definition of the production function. If this function is linear in the individual's decision variable, a rational individual only chooses between not contributing to the public good at all, or contributing maximally. By the definition of the dilemma, the former prediction holds. If, by contrast, the production function is nonlinear, the individual's best response is no longer at the corner, but in the interior of the action space. With this change in the production function the dilemma does not go away. The good is still underprovided, to the bad is overprovided. The

the public good regardless of whether they invest in creating it, each individual has an incentive to free ride.[182] Taken to its natural conclusion, this means that although each person would be better off (as a member of society) if the public good were produced, each person will choose—as is predicted by neoclassical economic theory—to maximize her own wellbeing (as an individual) by not participating.[183] The same goes for a public bad. If each individual benefits from not suffering the bad, but earns individual income from activity that contributes to that bad—and that income exceeds the allocated share of the public bad caused by contribution that the individual does suffer—then each individual will contribute to the public bad *even though* the existence of the public bad harms everyone, including that individual.

The logic of this point is worth stressing. In a social dilemma, defection—by free riding on a public good, or contributing to a public bad—is a dominant strategy.[184] Cooperation, defined as contributing to a public good, or refraining from contributing to a public bad, is socially optimal, but an inferior strategy from the individual perspective. If an individual seeks to maximize her own benefit, she will defect irrespective of her expectations about others' behavior. If she believes that some or all others will cooperate, she is still best off defecting. She enjoys the public good provided by the contributions of others, and additionally enjoys the benefit from not having to contribute. If, by contrast, she believes that all others will defect, she will follow suit. If she were to be the only one to cooperate, she would be even worse off. She would not enjoy the public good in its entirety, but would lose the benefit of not having to contribute. The fact that defection is a dominant strategy follows from the production function that defines the public good. For the individual, her own contribution to the public good has a benefit smaller than the cost.

---

individual only stops going to the extreme because damage on her would be too high. Classic illustrations of nonlinear production functions are quadratic. They are typical for harvesting natural resources beyond sustainability.

182. *See id*.

183. *See id*. at 415 ("So, unless the incentive structure changes, for example by charging user fees, self-interested individuals will not cooperate in the production of public goods even if each would obtain net benefits if those goods were produced.").

184. *See* Ledyard, *supra* note 10, at 113.

B. Privacy is a Public Good

Translated to privacy, the public-goods model assumes that at least some individuals calculate the following way: If I disclose information, I will receive a private benefit—access to an online site or service, for example. This imposes a cost on me, based on the personal information I have given up, and it imposes a cost on everyone because I have contributed to the overall lack of privacy in the culture. Yet as long as the sum of my direct costs and my share of the social costs (resulting from my own release of private information) is less than the private benefit I gain, I will choose to give up information to access the site or service.

Thus, it makes sense to examine privacy as a social construct, subject to the problems of social production.[185] Indeed, we contend that privacy is a public good as that term is strictly defined in the economics literature. Privacy will fall prey to social dilemmas. In 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.

One way to perceive the problem clearly is to consider lack of privacy as a public bad, to which we all contribute when we post information about ourselves that generates negative spillover effects. Recall that public goods and public bads are mathematically identical, with only the framing of the problem changing. The production function for clean air can be expressed as the minimization of the production function for creating pollution. This framing switch is a powerful tool for understanding how privacy is a public good. It is much easier to perceive the problem using the public-bads model.

1. *The Public Bad of Lack of Privacy*. Online, individuals regularly face the following decision: they are invited to join some Internet platform, knowing (more or less vaguely) that they will indirectly pay by making personal information available. Take the typical social network. The individual damage a user foresees when leading an active online life seems reasonable. A user might reason that the likelihood of negative consequences is low, and even if an

185. Cohen, *supra* note 2, at 1908 ("The self has no autonomous, precultural core, nor could it, because we are born and remain situated within social and cultural contexts. And privacy is not a fixed condition, nor could it be, because the individual's relationship to social and cultural contexts is dynamic.").

event were to occur, it likely would not be momentous. The user may not perceive individual risk sufficient to stimulate abstention from the immediate and personal benefits conveyed by use of the network. The user knows she will reveal some information about her friends and family. Maybe the user knows one of them to be particularly vulnerable, but does not account for the risk of her own contributions to data about that person—few people understand or even consider that a message of sympathy in the event of illness might affect healthcare premiums.

This is precisely the kind of reasoning the public-bads model aims to capture. The user's anticipated individual damage is too small to outweigh anticipated benefit. Things would look differently if users were to factor in the negative repercussions of being generous with their private information on the privacy risk faced by others and vice versa. Yet as long as each user only considers the potential damage to herself, no individual would be concerned that anticipated damage outweighs actual and anticipated benefit. If, however, 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.

Information-based public bads are 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 a function of rising data storage and parsing. Technological increases in storage capacity and in the predictive power of machine analytics undermine incentives to seek privacy. Little is forgotten, and stored information can be put to ever-greater uses. Storage has now increased so dramatically that the sum of all recorded human information available in 2007 is merely a minute fraction of the information stored and parsed today.[186] Search algorithms are now sufficiently advanced that this increased volume of data does not act to obscure, but instead increasingly reveals information about subjects.[187] Individuals are less and less able to

186. Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981, 998 (2014).

187. *See* Scott Shane, *Data Storage Could Expand Reach of Surveillance*, N.Y. TIMES: THE CAUCUS (Aug. 14, 2012, 5:50 PM), http://thecaucus.blogs.nytimes.com/2012/08/14/advances-in-data-storage-have-implications-for-government-surveillance [https//perma.cc/K7M5-TZYB] ("Government at every level is experimenting with sophisticated surveillance equipment whose capabilities are improving as rapidly as every other kind of electronic technology. . . . It will

control and monitor the damage that their revelations may cause to themselves, let alone to others. Small contributions to the data pool provide bigger results. Individuals 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. No wonder, then, that even the most privacy-minded consumers may eventually defect.

Treating privacy as a public good thus goes a long way toward explaining the central conundrum of commercial privacy—why it is that consumers claim to want privacy, but do not refuse valuable goods and services that come at a significant privacy cost to both themselves and others. We reject the facile answer that consumers are lying about privacy preferences. The answer is that they believe that due to the actions of society as a whole, they have no choice and no privacy anyway. Under those circumstances it makes sense to give up privacy-seeking behavior and seize what private benefit they can.

2. *Mapping Social Harm*. A key element of treating privacy as a public good is that law must be able to recognize the social and systemic harms caused by the collection, aggregation, and exploitation of data. Courts tend to focus on specific harm to specific complaining individuals, not undivided losses to social welfare.[188] Economists have a different sense of harm.[189] Translating allocated social-welfare harms into actionable legal rules will therefore require patience and creativity.

One question is whether group privacy harms can be sufficiently theorized to be legally cognizable.[190] Early data-breach cases were often dismissed on the grounds that plaintiffs had not yet suffered any harm, because they could not show that their data had yet been

soon be technically feasible and affordable to record and store everything that can be recorded about what everyone in a country says or does.").

188. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1148–49 (2013) (holding that the plaintiffs failed to demonstrate that the future injury they purportedly feared was (1) certainly impending and (2) fairly traceable to the Foreign Intelligence Surveillance Act provision at issue—specifically, a provision that allowed surveillance of individuals who were not "United States persons" and were reasonably believed to be located outside the United States).

189. Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1061, 1062 (2009).

190. *See* MacCarthy, *supra* note 1, at 456–68 (describing evolving categories of harm related to information externalities).

improperly used.[191] As one court concluded, "[p]laintiffs lack standing because their claims are future-oriented, hypothetical, and conjectural. There is no 'case or controversy.'"[192]

It has therefore taken some time to convince courts to sanction even direct, individual examples of data harm.[193] The trend is promising, however. Thus, "[t]he more recent trend . . . suggests that in 'lost data cases,' an increased risk of harm, e.g., the risk of identity theft, is an injury-in-fact sufficient to confer standing."[194] On the other hand, the Supreme Court expressed skepticism in *Clapper v. Amnesty International*[195] about whether plaintiffs who cannot show that surveillance harm is "certainly impending" can sue.[196]

Diffuse harms of the kind caused by public bads take significantly more theory and experience to define than do direct and individual harms. For example, it is commonplace for an institution to suffer a data breach, yet to claim that no harm was done unless the data is actively misused in individual cases. Courts do not give much

191. *See* Allison v. Aetna, Inc., No. 09-2560, 2010 WL 3719243, at *6 (E.D. Pa. Mar. 9, 2010); Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1050 (E.D. Mo. 2009) (finding no injury-in-fact in the mere possibility of identity theft); *In re* TJX Cos. Retail Sec. Breach Litig., 246 F.R.D. 389, 400 (D. Mass. 2007); Kristen Blanchette, *Civil Litigation: Security*, *in* 1 DATA SECURITY & PRIVACY LAW § 8.27 (Ronald N. Weikers ed., 2015) ("Putative class action lawsuits for large scale data breaches are often dismissed during the initial stages of the litigation because the plaintiffs failed to allege an injury-in-fact and, therefore, lack standing to sue.").

192. Hammond v. The Bank of N.Y. Mellon Corp., No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *7 (S.D.N.Y. June 25, 2010); *see also* Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011) (holding that plaintiffs lacked standing to bring suit against defendant corporation after defendant suffered a security breach of plaintiff's information); Lambert v. Hartman, 517 F.3d 433, 437 (6th Cir. 2008) (reviewing defendant's claim that plaintiff lacked standing to bring suit after defendant published personal identifying information from traffic citation on its website); Robert D. Brownstone & Tyler G. Newby, *Privacy Litigation*, *in* 1 DATA SECURITY & PRIVACY LAW, *supra* note 191, § 9:159 ("A frequent defense against various privacy theories, including common law, is that the plaintiff has failed to allege an 'injury-in-fact' sufficient to satisfy the standing requirement of Article III of the U.S. Constitution.").

193. *See* Gavin Brody, *DOD, Tricare Claim No Harm, No Foul in Data Theft Case*, LAW360 (Nov. 20, 2012, 5:31 PM), http://www.law360.com/articles/395323/dod-tricare-claim-no-harm-no-foul-in-data-theft-case [http://perma.cc/TJF9-3LZ4] (reporting on this issue in the context of a data breach that affected 4.9 million Tricare beneficiaries).

194. *See* Anderson v. Hannaford Bros. Co., 659 F.3d 151, 166–67 (1st Cir. 2011); McLoughlin v. People's United Bank, Inc., No. 3:08-cv-00944(VLB), 2009 WL 2843269, at *4 (D. Conn. Aug. 31, 2009); Blanchette, *supra* note 191, § 8:28 (discussing *Pisciotta v. Old National Bancorp*, 499 F.3d 629 (7th Cir. 2007)).

195. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

196. *Id.* at 1143.

weight to the increase in systemic risk occasioned by the breach.[197] Yet such systemic harms almost certainly exist. One straightforward example of social-data harm is the increase in systemic risk of identity theft.[198] The data pools created by companies are prime targets.[199] When an organization or company loses this information, the costs are not borne merely by individuals, but by affected members of the system and social groups. For example, a child of one of the authors was a victim of the Anthem Health Data hack, requiring the author to expend significant amounts of time and effort to contain the results.

In response, the legal culture has begun to recognize the social harms resulting from data breaches.[200] Law has also begun to respond, not only to the individual harms, but also to the allocated social harms of data practices. The theft of one piece of data is now more dangerous, because it can be used to link to other pieces.[201] Of course, obtaining additional pieces of data further simplifies the identity thief's objective.

---

197. *See* Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep Up with Technological Change*, 7 U. ILL. J.L. TECH. & POL'Y 239, 239 (2007) ("It is often stated that the law lags behind technology. As technology changes and creates new possibilities, lawyers and legal scholars struggle to deal with the implications."); John Burn-Murdoch, *Data Protection Law is in Danger of Lagging Behind Technological Change*, THE GUARDIAN (Apr. 12, 2013, 7:25 AM), http://www.theguardian.com/news/datablog/2013/apr/12/data-protection-law-lagging-behind-technology [http://perma.cc/22CB-AZD6] ("Data processing practices are evolving faster than the law can adapt to them, according to a senior British lawyer at an international law firm specialising in data protection.").

198. *See* J. Craig Anderson, *Identity Theft Growing, Costly to Victims*, USA TODAY (Apr. 14, 2013, 4:38 PM), http://www.usatoday.com/story/money/personalfinance/2013/04/14/identity-theft-growing/2082179 [http://perma.cc/4F6K-JENN] ("[I]dentity theft has become big business. The number of malicious programs written to steal your information has grown exponentially to an estimated 130 million from about 1 million in 2007.").

199. *See id.* ("The most successful identity thieves have learned that it's more lucrative to hack into businesses, where they can steal card numbers by the thousands or even millions.").

200. *See*, *e.g.*, Anderson v. Hannaford Bros. Co., 659 F.3d 151, 167 (1st Cir. 2011) ("Plaintiffs' claims for identity theft insurance and replacement card fees involve actual financial losses from credit and debit card misuse. Under Maine contract law, these financial losses are recoverable as mitigation damages so long as they are reasonable."); Ruiz v. Gap, Inc., 380 F. App'x 689, 691 (9th Cir. 2010) ("[G]reater risk of identity theft presents enough of a risk that the concerns of plaintiffs are real, and not merely speculative."); *see also* MacCarthy, *supra* note 1, at 481 ("Harm can be probabilistic. Extra risk of harm is also a harm. . . . The increased risk of identity theft is a measurable harm.").

201. This point is forcefully argued by James Fallows, *Hacked!*, THE ATLANTIC MAG. (Nov. 2011), http://www.theatlantic.com/magazine/archive/2011/11/hacked/308673 [http://perma.cc/F9ZN-NYFF].

Thus, the trend has also begun to shift in class actions. In a 2015 case, *Remijas v. Neiman Marcus Group, LLC*,[202] the Seventh Circuit held that the class of plaintiffs met the pleading requirements for standing in a class action responding to a hacking breach of retailer Neiman Marcus—the closest the litigation system has come to capturing group harms.[203] The *Remijas* court noted that mitigation costs incurred by plaintiffs in response to a perceived, speculative, and remote harm were often insufficient to permit a plaintiff class to recover, but reframed the loss of personal data as posing a much more concrete risk.[204] In distinguishing *Clapper*, the Seventh Circuit noted:

> Clapper was addressing speculative harm based on something that may not even have happened to some or all of the plaintiffs. In our case, Neiman Marcus does not contest the fact that the initial breach took place. An affected customer, having been notified by Neiman Marcus that her card is at risk, might think it necessary to subscribe to a service that offers monthly credit monitoring. It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014. It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded.[205]

States have also been engaging in a concerted regulatory response to combat systemic risks. The theory upon which much of the recent state regulation has been based is that requiring companies to reveal data breaches, often regardless of whether the data has been used in the individual case, will permit consumers, insurers, and defensive-software designers to mitigate systemic risk. In recent years nearly every state has enacted breach-notification laws, and there is a push for federal legislation on the topic.[206]

---

202. Remijas v. Neiman Marcus Grp., LLC, No. 14-3122, 2015 WL 4394814 (7th Cir. July 20, 2015).

203. *Id.* at *5.

204. *See id.*

205. *Id.*

206. *See Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [http://perma.cc/7EDG-KVBF] ("Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information.").

Notification is merely a first step toward addressing systemic social risk. A systematic and easily understandable account of the social costs of privacy failures is critical in order to move forward. Law often lags in setting definitions and boundaries for social harms, and the data context is no exception.[207] Theory and science are needed to advance the ball. In the twentieth century, for example, law lagged the science of the social costs of cigarette smoking or using products like asbestos. The first cases were ones of direct harm.[208] Later theory and science established harm to wider categories of people impacted by smoking or asbestos, even exposures to secondary effects decades later.[209] Similarly, it is reasonable to expect that, as legal theory and data science develop, increasingly temporally distant and distributed data harms will become increasingly distinct and legally cognizable.[210]

Data pollution causes other social harms that, while demonstrable, may need to be addressed outside of the individual-centered forum of courts.[211] For example, behavioral models derived from consumer data do permit more deals to close, but they also permit companies to extract nearly all of the consumer surplus.[212] The resulting wealth transfer is supposed to be worth efficiency gains, but given declining marginal utility of wealth and the difference in wealth levels between companies and consumers, these gains may actually be social losses, especially if consumers suspect exploitation. Advertising relies on models trained on large amounts of information, which then

207. MacCarthy, *supra* note 1, at 456–68; Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1736 (2010).

208. *See* Borel v. Fibreboard Paper Prods. Corp., 493 F.2d 1076, 1082 (5th Cir. 1973) (en banc) (affirming the panel's decision that the plaintiff, an insulation worker, was entitled to go to jury on the question of whether his injuries due to asbestos exposure were voluntary or a result of unreasonable duress of circumstances).

209. *See* Jackson v. Johns-Manville Sales Corp., 750 F.2d 1314, 1336–37 (5th Cir. 1985) ("[N]ew groups of plaintiffs from different points along the line of distribution of asbestos are emerging. Potential claimants include warehouse workers, truck drivers, longshoremen, and spouses of workers exposed when the worker returned home covered with asbestos dust.").

210. *See* Ohm, *supra* note 207, at 1733–35 (describing the history of privacy law and the current shift to preventing harm caused by Personally Identifiable Information (PII)).

211. *See* Remijas v. Neiman Marcus Grp., LLC, No. 14-3122, 2015 WL 4394814, at *5 (7th Cir. July 20, 2015) ("For the sake of completeness, we comment briefly on the other asserted injuries. They are more problematic. We need not decide whether they would have sufficed for standing on their own, but we are dubious.").

212. *See* BERNASEK & MONGAN, *supra* note 68, at 17; Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, WALL ST. J. (Aug. 23, 2012, 6:07 PM), http://www.wsj.com/articles/SB10001424052702304458604577488822667325882 [http://perma.cc/9ZB4-YZ28] ("[T]he online travel agency is starting to show them different, and sometimes costlier, travel options than Windows visitors see.").

can be quickly matched to what an advertiser knows about a specific individual. The more information available, the more accurate the advertisement model is.[213] Consider the mechanism behind advertising selection. When a user enters a website, some parts of the site support advertisements. Those advertisements are targeted by means of a rapid, behind-the-scenes auction, in which the parties who wish to advertise to the user attempt to determine how much that user's attention is worth to them.[214] The better the match between the user's proclivity to buy and the advertisement on offer, the higher the price.[215] Person A's contributions to the fine-tuning of the advertisement model therefore impact Person B, and do so in a way that Person A is not likely to fully grasp or deceives her outright. The more the advertising company knows about the potential customer, the better its ability to confront the customer with a message she is very unlikely to resist.[216]

A further important appeal of data mining does not result from targeted advertising, but from targeting the actual offer. Behavioral models derived from consumer data drive up prices.[217] For most products, consumers' willingness to pay varies widely, both between and within consumers. Some consumers crave the new product, while others would only buy at a price that equals the marginal cost of producing another unit. And most individuals cherish the first unit of the new good much more than any additional unit. The more a provider knows about a customer's preferences, income, wealth and

213. *See* Doug Henschen, *Analytics Gets More Accurate, More Accessible*, INFO. WEEK (Nov. 15, 2012, 5:10 PM), http://www.informationweek.com/big-data/big-data-analytics/analytics-gets-more-accurate-more-accessible/d/d-id/1107416? [https://perma.cc/249Y-7S9P] ("The more data companies use, the more accurate their predictions become.").

214. *See Ad Targeting: About the Ad Auction*, GOOGLE ADSENSE, https://support.google.com/adsense/answer/160525?hl=en [https://perma.cc/MZ8G-VXW3] ("[O]ur ad auction allows advertisers to state the price they're willing to pay for clicks on ads or for impressions served on AdSense pages.").

215. *See Ad Targeting: About Smart Pricing*, GOOGLE ADSENSE, https://support.google.com/adsense/answer/190436?hl=en&ref_topic=1628432 [https://perma.cc/BW2R-JQSC].

216. Note that we depart from economic orthodoxy in that we do not consider pure seller price discrimination to be an undivided good. Perfect price discrimination is often seen as a route to economic efficiency, permitting sellers to offer the cheapest deals to those who can pay the least. Yet it is not—it merely ensures that the seller captures value that would otherwise inure to the consumer as consumer surplus. Given the well-established declining marginal value of wealth, we do not see wealth transfers from consumers to corporations in the data market to maximize overall welfare. *See* Matthew A. Edwards, *Price and Prejudice: The Case Against Consumer Equality in the Information Age*, 10 LEWIS & CLARK L. REV. 559, 592 (2006) (discussing perfect price discrimination and efficient outputs).

217. *See* BERNASEK & MONGAN, *supra* note 68, at 92–98.

consumption patterns, the better it can exploit her by offering the product at a price that this customer, in this situation, still finds acceptable.[218] Often the provider has yet another degree of freedom. It can customize the product itself, and make this customer an offer that is just too good to resist. The customized product certainly gives the consumer additional value; otherwise she would not buy it. But the producer engages in customization because she stands to gain much more than the consumer.[219] In the technical language of microeconomics, the producer aims at appropriating the lion's share of what, with a standardized product, would have been the consumer's rent.[220]

The former outcome is of course a classic of microeconomic theory, and is known as perfect price discrimination. The latter can be referred to as perfect product differentiation: each customer gets a personalized product that perfectly matches her preferences. In the pure world of economic models, perfect price and product discrimination only raise an issue of distributional justice. Producers have found a way to appropriate the total social surplus. Efficiency still obtains. Yet one reaches this result only if consumers are willing to accept any small gain, even if it is grossly inequitable. A standard result from experimental economics shows that this assumption is likely incorrect. The situation is akin to an ultimatum game. In this game, a proposer has power to make a take-it-or-leave-it offer for splitting an amount of money received from the experimenter. If the offer is rejected, the endowment is forfeited. If the responder indeed maximizes profit, the proposer may leave the responder with the smallest positive increment, and keep the remainder for herself. Yet in the lab, such offers are almost surely rejected. Experimental participants would rather burn money than let the proposer exploit them.[221] The same is to be expected with producers using perfect product differentiation to exploit consumers. If this is what happens, not only do individual consumers suffer, but society at large suffers

218. *Id.*

219. *Id.* at 108–113.

220. *Id.*

221. *See generally* Werner Güth, Rolf Schmittberger & Bernd Schwarze, *An Experimental Analysis of Ultimatum Bargaining*, 3 J. ECON. BEHAV. & ORG. 367, 382 (1982) ("[P]layers 2 are willing to suffer a monetary loss if they consider the demand of player 1 as unacceptable."). For a meta-study of the burgeoning experimental literature using this game, see generally David J. Cooper & E. Glenn Dutcher, *The Dynamics of Responder Behavior in Ultimatum Games: A Meta-Study*, 14 EXPERIMENTAL ECON. 519 (2011).

along with them. A "deadweight loss" results from the fact that a relevant portion of demand that could have been served at prices below marginal cost actually never buys.

Big data harms go well beyond user risk or consumer exploitation. Lack of privacy also harms the body politic, and therefore some remedial efforts must be political.[222] Privacy is important to basic democratic processes.[223] It is important for independent decision making.[224] Privacy has been described as a human right, although this perspective has received more focused attention in Europe than in the United States.[225] Even in the United States, the revelations of Edward Snowden show the potential danger of unrestricted corporate gathering of consumer information.[226] The large amount of information gathered by companies was placed at the disposal of the NSA through the PRISM program.[227] Other news revelations have focused on metadata collection. The telephony-metadata collection typified by the Verizon Order appears to rely on the collaboration of telecommunications intermediaries to hand off information routinely gathered in the course of operation of the company.[228] Under the order, Verizon (and other companies, it is safe to assume) must hand off this information to government actors on an

222. *See* Solove, *Privacy*, *supra* note 64, at 1153 ("[A] conception of privacy that view[s] it as a discrete harm, akin to a tort harm . . . is a constrained way to view the disruption created by the aggregation and uncontrolled uses of personal information by private sector bureaucracies. This disruption of the way that power is allocated between individuals and large corporations goes to the structure of our society as a whole.").

223. *See* Schwartz, *Privacy and Democracy*, *supra* note 108, at 1649 ("From the civic republican perspective, the true promise of the internet will not be as a place for electronic commerce, but as a forum for deliberative democracy.").

224. *See id.* at 1656.

225. Robin D. Barnes, *The Caroline Verdict: Protecting Individual Privacy Against Media Invasion As A Matter of Human Rights*, 110 PENN ST. L. REV. 599, 599 (2006).

226. *See, e.g.*, Mark Mazzetti & Michael S. Schmidt, *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance*, N.Y. TIMES (June 9, 2013), http://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html?_r=0 [http://perma.cc/4XVZ-HC64] (discussing the backdrop to, and possible ramifications of, Edward Snowden's disclosure of classified intelligence information).

227. *See* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 6, 2013), http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers [http://perma.cc/L9HS-NGPY].

228. *See* James Ball, *Verizon Court Order: Telephone Call Metadata and What It Can Show*, THE GUARDIAN (June 6, 2013, 10:12 AM), http://www.theguardian.com/world/2013/jun/06/phone-call-metadata-information-authorities [http://perma.cc/8LP3-AGWP] (discussing U.S. government collection of telephony metadata retained by telecommunications service providers).

ongoing and forward-looking basis. Pervasive government surveillance is not a positive democratic or humanitarian value. The damage is both personal and social. Citizens have begun to censor themselves online.[229] Surveillance has already chilled discourse.[230] Socially, large pools of corporate-gathered data damage the societies that generate them.[231]

Throughout, evidence suggests a slow evolution of law and theory from a sense of the individual damage of loss of privacy to its social cost. This Part therefore concludes that privacy and public-goods models fit together with respect to the harms caused. Individual contributions both yield a private benefit (ostensibly free services) and negatively impact others' privacy. Individual incentives to protect privacy track individual incentives in a public-goods model. The lack of privacy which results from the social dilemma corrodes further attempts to cooperate as people become discouraged, see others give in, and observe the growing strength of data mining. In each of these ways and more, pooled data harms citizens individually, in groups, and as a body politic. We are therefore confident that privacy harms track those recognizable from public-goods analysis.

III. APPLYING PUBLIC-GOODS THEORY TO PRIVACY PROBLEMS

In this Part, we draw on the broad and untapped neoclassical- and behavioral-economics literature to seek new paths for the legal debate over privacy. As noted above, that debate does not adequately account for negative externalities on others resulting from disclosing private information. This Part therefore explores and tests solutions developed in the neoclassical- and behavioral-economics literature to ascertain the degree of useful fit for the social dilemma of privacy.

---

229. *See* Sauvik Das & Adam Kramer, *Self-Censorship on Facebook*, *in* PROCEEDINGS OF THE SEVENTH INTERNATIONAL CONFERENCE ON WEBLOGS AND SOCIAL MEDIA 120, 125 (2013), http://www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/viewFile/6093/6350 [http://perma.cc/8DW9-CMT5] (finding that 71 percent of Facebook users engaged in last-minute self-censorship).

230. *See, e.g.*, BJ Ard, *Confidentiality and the Problem of Third Parties: Protecting Reader Privacy in the Age of Intermediaries*, 16 YALE J.L. & TECH. 1, 8 (2014) (arguing that, in an increasingly digitized age, the current regime's protection of providers of reading material, such as libraries, rather than protecting the reading material itself, leaves gaps in intellectual privacy when readers procure their materials from third parties like Amazon).

231. *See, e.g.*, ARTHUR R. MILLER, THE ASSAULT ON PRIVACY 207 (1971) (noting that with "electronic surveillance, the climate or atmosphere of suspicion created by an accumulation of invasions of privacy is of far greater concern than the direct harm caused by the incidents themselves").

Because we chiefly suggest normative approaches based on experimental results, some caveats are in order regarding the nature of experiments. Experiments do not attempt to describe what a thing is, but rather how one factor operates in conjunction with others.[232] Experiments provide two important advantages: they "make it possible to study phenomena that are hard, if not impossible, to observe in the field," and they allow experimenters, through randomization, to solve what empirical social scientists tend to call identification problems.[233] A typical experiment consists of a baseline and a treatment. Participants are randomly assigned to either condition. Baseline and treatment differ by one, and only one, feature of the design. On these conditions, a significant difference between the baseline and the treatment is proof that the one difference in design causes the difference in outcome.[234] Because experiments seek to narrow the range of interaction, they do not capture every feature available. Indeed, they must exclude any other variable that could confound the result. It is therefore not a strong criticism to point out that an experiment has left something out, especially something that would have altered the experiment's outcome. That is what experiments must do.

This rigorous approach does leave a gap, however. Experimentalists generally refrain from offering normative or policy approaches grounded in their work, largely because some of the factors that have been left out to solve the identification problem may comprise important parts of the policy problem. This is where legal analysis and theory can provide some help. Lawyers fit studies to cases. They are skilled contextualists, trained to focus on the elements of different contexts that make the difference between different cases. Thus, while it might be unseemly for scientists to make normative suggestions based on their individual experimental findings, it is necessary for policy makers—and this includes legal theorists—to engage with the policy implications of the research. This is all the more necessary because legal theorists often overindulge in theory at

232. *See* Christoph Engel, Legal Experiments—Mission Impossible? 7 (June 9, 2013) (unpublished manuscript), http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2276566_code251559.pdf?abstractid=2276566&mirid=1 [http://perma.cc/BD54-FGGZ].

233. *Id.* at 1, 7.

234. *See id.* at 7.

the expense of checking intuitions against data generated in carefully controlled experiments.[235]

This Part attempts to express the best of both worlds. It draws on the past several decades' worth of experimental evidence on group coordination in the face of social dilemmas before pushing beyond the narrow findings of experiments to suggest normative approaches that might improve privacy protection for groups. We suggest potentially useful new approaches to a field of study that has a tendency to become mired in ontological debates. The purpose is not to suggest that the economic and experimental literatures lead ineluctably to these conclusions. Rather, the literature points the way toward possible solutions that have been unexplored or underexplored. This is the pleasant task of an early mover in a given subject: to point out what might work.

A. Repeated Interaction

Repeat play is a critically important feature impacting coordination on group welfare. If two anonymous individuals meet once, it may be that standard economic theory gets it right, and each may act selfishly (although query, then, why people usually tip waiters). These two individuals have no reason to care for each other, other than the circumstances under which they meet. The economic theory of public goods is just a rigorous way of defining these circumstances. Economists model these circumstances as a game. Players best respond to what they know or expect the other player to do. If this game is a dilemma, players need not even go that far. Whatever the other player decides to do, they maximize their personal payoff by misbehaving. In some respects, this is an adequate model for the problem of online privacy. A world of strangers is one in which I am unlikely to encounter someone again in a way that my past track record or future cooperation will matter.

Yet the Internet is not purely organized out of an undifferentiated mass of strangers, but rather nested smaller groups with higher frequencies of repeat play.[236] Within such nested groups,

235. *See* Lee Epstein & Gary King, *The Rules of Inference*, 69 U. CHI. L. REV. 1, 9 (2002) ("Too much legal scholarship ignores the rules of inference and applies instead the 'rules' of persuasion and advocacy. These 'rules' have an important place in legal studies, but not when the goal is to learn about the empirical world.").

236. *See* Kosinski et al., *supra* note 131, at 5802 (noting, for instance, how "location within a friendship network at Facebook was shown to be predictive of sexual orientation").

people may reasonably consider the impact defections may have on others' future incentive to cooperate. If I post an embarrassing picture of my friend on Facebook, she might do the same to me tomorrow. In such situations, it is more plausible to model the interaction as a repeated game. Typically it will be appropriate to think of a game that does not have a precisely defined, ex ante known end. If one seeks to induce cooperation in groups, this is good news. A repeated game with an unknown end entails a credible shadow of the future. If it becomes known that I have misbehaved by recklessly sharing dangerous information, others may sanction me, or simply start doing the same.[237] The value of future cooperation may sustain present cooperation.

However, if the end of the game is known in advance, then the theoretical prediction of cooperation changes. In the real world, counterparties rarely know with perfect certainty when a relationship ends. But some situations at least come close. Consider how a disgruntled employee's incentives shift once she has given two-weeks notice. Unless she expects a positive letter of recommendation, she is unlikely to make personal sacrifices for the good of the firm. Worse, she may actively act in her own best interests against the interests of the group, by erasing data, or taking valuable information with her to start a competing business. This is a textbook "final period problem," in which groups decohere when members know they will obtain little or no benefit from their continued cooperation.[238] Imagine that a player considers whether to defect or cooperate in a public-bads game. The player would determine whether to defect by contributing to the public bad, for which she receives a personal profit, or refrain from contributing, which means that she only keeps her endowment. She may decide to cooperate because the future benefits of cooperation outweigh the single-turn payout she receives from defecting. In the last round of the game, however, she no longer has

237. Game theorists refer to this result as the "folk theorem." *See generally* Robert Aumann & Lloyd Shapley, *Long Term Competition—A Game Theoretic Analysis*, 14 ANNALS ECON. & FIN. 609 (2013) (discussing game-theoretic models of cooperation between competitive actors when iterated interactions present the possibility of future benefits from present cooperative behavior). For an application of the folk theorem to a public good, see generally Kreps et al., *supra* note 48.

238. *See* JESSE H. CHOPER, JOHN C. COFFEE JR. & RONALD J. GILSON, CASES AND MATERIALS ON CORPORATIONS 566–67 (6th ed. 2004) ("In this 'end game,' there is greater reason for managers to act opportunistically. . . . Economists call this a 'final period' problem, referring to the fact that the agent no longer has the same incentives to serve the principal faithfully.").

an incentive to invest in the future, and will defect. Cooperation will disintegrate as players realize that defecting earlier and earlier is a more profitable option, especially if they expect others do the same.[239] By this process, termed "unraveling," neoclassical economics predicts that players will defect from the very first round on.[240]

Behavioral economists have discovered some interesting tools for dealing with unraveling.[241] The certainty that a relationship will end does not seem to matter as long as counterparties are uncertain as to when.[242] If the likelihood of the game ending at any given point is random—that is, the game may end each round but it does not do so with certainty—then cooperation can be sustained in the face of unraveling. Players can sustain cooperation when they no longer know exactly when a mutually beneficial relationship will come to an end.

A closely related phenomenon is that players may consider the chance of other players defecting. This could either be defection in response to the defection of the deciding player, or it might be outright defection given the incentives the group faces. A player will cooperate if a game has a certain length, and she does not expect other players to exploit her with certainty. As a matter of fact, cooperation can be sustained if the deciding player believes that other players might defect, but the game is long enough that the benefits of future cooperation are worth the risk. Thus, cooperation is sustainable in groups when the endpoint of cooperation is not previously established and when other people do not expect necessarily to be exploited.

There is also cause for optimism because the experimental literature does not support the theoretical prediction of unraveling and complete defection, even when there is a known game end. In experiment after experiment, group members are willing to cooperate at the beginning, but learn over time to defect, because cooperation is

239. *See* Hans-Theo Normann & Brian Wallace, *The Impact of the Termination Rule on Cooperation in a Prisoner's Dilemma Experiment*, 41 INT'L. J. GAME THEORY 707, 709 (2012).

240. *See, e.g.*, *id.* at 708; Robert W. Rosenthal, *Games of Perfect Information, Predatory Pricing and the Chain Store Paradox*, 25 J. ECON. THEORY 92, 92–99 (1982) (theorizing that a rational player will take an immediate payoff that ends the game, rather than continuing to play for a possibly higher payoff, because the player assumes his opponent is also rational and would do the same); Selten, *supra* note 48, at 130–33.

241. *See* Normann & Wallace, *supra* note 239, at 708–11 (describing a variety of approaches to game termination designed to address cooperation issues that arise in prisoner's-dilemma games).

242. *See id.* at 708–09.

punished in a social dilemma.[243] This suggests that people come to social dilemmas with life experiences or cultural commitments that make them predisposed to cooperate at higher rates than neoclassical economics would predict.[244] This is likely because people know from experience that they cannot predict when another person may impact their life. Cooperation as a default is a response to the general unpredictability of social life.

Repeat play can produce cooperation as long as the end of the game is not known with certainty, and in experiments, subjects demonstrate a willingness to cooperate early on even where the game end is known. However, repeat play can also corrode cooperation through the repeated experience of being punished by the social dilemma. Absent some form of institutional backing, cooperation is not stable. The longer participants unsuccessfully interact, the more cooperation decreases.[245]

Effective application requires accounting for each of these effects. Fostering repeat play among more tightly knit online groups may foster cooperative behavior and reduce intentional malicious disclosures. On the other hand, repeated fruitless attempts to protect privacy are likely to induce an effect akin to learned helplessness.[246]

Applying this insight to privacy, we note that features that remind users of the value of cooperation given the shadow of the future are built into social networks, but they are not ones commonly expected to produce privacy gains. First, certain aspects of social networks act to remind users that they are repeat players. Friends of friends appear on personal walls. Routine "Do you know x? He is a friend of y." reminders are sent out by the social networks in order to encourage users to expand their personal networks.[247] Social networks

---

243. *See* Ledyard, *supra* note 10, at 146–47 (surveying experimental evidence of decrease in contribution to public good by repetition).

244. For a study of cultural constraints that produce ordered systems without government intervention, see ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES 123–27 (1991).

245. *See* Blair & Stout, *supra* note 42, at 1763 ("[E]xperimental studies show . . . [that] cooperation rates are lower in reiterated play than in one-shot games.").

246. *See* Steven F. Maier & Martin E. Seligman, *Learned Helplessness: Theory and Evidence*, 105 J. EXPERIMENTAL PSYCHOL. 3, 3 (1976) ("[T]he learned helplessness hypothesis . . . argues that when events are uncontrollable [an] organism learns that its behavior and outcomes are independent, and that this learning produces the motivational, cognitive, and emotional effects of uncontrollability.").

247. *People You May Know*, FACEBOOK, https://www.facebook.com/help/501283333222485 [http://perma.cc/MBY8-3NP7].

routinely scrape email lists, for example, to permit users to re-create their network of contacts within the network. These low-level reminders of the connection group members have with one another need not be limited to the moment a user joins the network. One might imagine a "featured contact" widget that serves to remind users of contacts with whom they have not spoken in some time, thus raising the perception of repeat play at the edges of an individual's network. Even more valuable, given the insights regarding inequity aversion and reciprocity below, would be aggressive promotion of the privacy-seeking actions others are taking. In the same way that a network could inform a user that a friend is using or enjoying a movie, the network could inform a user that a friend is using an encrypted chat feature and has requested a key exchange. Even spreading "likes" of privacy-enhancing technologies would help.[248]

It should similarly be possible to ameliorate the corrosive effects of repeat play. One step would be to give full force to consumer expectations of privacy through simplified terms of service and opt-in permission each time the information is reshared or sold forward. Even simpler tools might assist, however. For example, users are already in part empowered to delink their social-network content from posts or unflag from photographs that purport to represent them. This means that although they cannot control viral outbreaks of content about them, they may have some ability to manage the degree to which others use their data without consent. Individual actions taken to minimize the damage of others' disclosures should provide users with strong, immediate feedback and verifiable results,

248. Such tools may align with the incentives of the social network. Providers are often willing to protect users' data from certain privacy threats because they monetize that data and want no competitors—examples would be Facebook's protection of user data from crawlers, *see* Grégoire Jacob, Engin Kirda, Christopher Kruegel & Giovanni Vigna, *PubCrawl: Protecting Users and Businesses From CRAWLers*, *in* PROCEEDINGS OF THE TWENTY-FIRST USENIX CONFERENCE ON SECURITY SYMPOSIUM 507, 507 (2012), https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final30.pdf [https://perma.cc/33X2-CDBN] ("In 2010, Facebook sued an entrepreneur who crawled more than 200 million profiles, and who was planning to create a third-party search service with the data he had collected."), or Google's use of strong encryption in response to the Snowden revelations, *see* Nicole Perlroth, *Experts Oppose Government Key to Encoded Data*, N.Y. TIMES, July 8, 2015, at A1 ("Technology companies including Apple, Microsoft and Google have been moving to encrypt more of their corporate and customer data after learning that the National Security Agency and its counterparts were siphoning off digital communications and hacking into corporate data centers.").

to avoid the corrosion engendered by repeated experiences of failure.[249]

B. Group Characteristics

This Subpart turns from an examination of repeated interaction to an analysis of the impact of group composition. The simple mechanism of the public-goods experiment divides individual from group incentives. The currently overexact focus of privacy theory on individuals should thus be supplemented with an understanding of how groups work. Thus, the observable characteristics of the group matter.[250] One cannot tell how an individual will act with respect to a given challenge—say, that of preventing pollution or providing privacy—without knowing the characteristics of the group in which she finds herself.[251]

For a starting point, we rely on John Ledyard's parsing of characteristics that seem to impact group behavior.[252] Ledyard identifies well over twenty characteristics that psychologists and experimental economists have examined for impact on group behavior.[253] Subsequent research has identified even more. We have the happy task of picking those that we believe will have the greatest bearing on privacy in the age of social media and big data, but our list is by no means exhaustive. The following Subparts therefore discuss a range of group characteristics that bear on groups' ability to

249. A legitimate although ultimately tangential question is whether companies would have the incentive to build such tools. We merely claim that these tools might work for groups, and do not argue who should make them. But we note that the Federal Trade Commission's (FTC) current approach is consistent with an implementation of our suggestions. The FTC has tended to leave space for self-regulation by suggesting approaches for incorporating pro-privacy features while sanctioning only marked cases of deception or unfairness. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 612–15 (D.N.J. 2014) (upholding the FTC's unfairness authority in the data-security context); *see also* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1411 (2011) ("In the United States, a recent staff report of the [FTC] describes a Proposed Framework with three main components: privacy by design, simplified consumer choice, and increased transparency of data practices."); Solove & Hartzog, *supra* note 126, at 667 (noting that the FTC has recently begun taking enforcement action against broken *expectations* of consumer privacy, rather than broken promises of privacy).

250. *See* Ledyard, *supra* note 10, at 113 ("Economic theory suggests that it may be possible to change the institutions by which group choices are made in a way that causes the outcome to be closer to the group optimum.").

251. *See id*. ("To know how to do that, however, requires anticipating how individual choices will change as the institutions change.").

252. *Id.* at 141–42.

253. *Id.* at 142–43.

cooperate, and which we think have some relevance to the policy debate surrounding online privacy.

1. *Size*. Because many online social networks are colossal, and because we intuit that group size affects the ability to coordinate to achieve group outcomes, group size is a natural place to start mining the literature for insights about social networks and privacy.[254] Social diffusion is popularly understood to reduce incentives to take individual, positive, costly action. The well-known murder of Kitty Genovese is often used as an example to demonstrate the impact of diffuse responsibility on an individual's incentive to help.[255] Each person thinks that someone else will surely help, and so no one does. Based on this intuition, early experimental efforts focused on the cooperative impact of increasing group size.[256]

The experimental findings both confirmed and challenged conventional wisdom. Although evidence supported the claim that increases in group size lead to decreases in the ability of the body to allocate resources efficiently—in this case, by securing enough contributions to a public good—they did not support the hypothesis that purely increasing numbers decreased group capabilities.[257] Instead, economists Mark Isaac and James Walker, who have tested this question in the lab, found that the less players received from cooperating (their marginal per-capita return, or MPCR), the less the players cooperated to produce the public good.[258] Provided the individual profitability of contributing to the public (the MPCR) is held constant, experiments yielded little evidence of a pure effect of group size. It appears that with a sufficient MPCR,[259] even large groups can produce public goods.[260] Later experiments by Isaac,

254. *See* R. Mark. Isaac & James M. Walker, *Group Size Effects in Public Goods Provision: The Voluntary Contributions Mechanism*, 103 Q.J. ECON. 179, 179 (1988).

255. *See* Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity As Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. MIAMI L. REV. 991, 1008 (2004) ("Research has shown that when large groups of people witness acts of violence or anti-social behavior, responsibility tends to diffuse among the witnesses.").

256. *See* Isaac & Walker, *supra* note 254, at 184.

257. *See id.* at 179–80.

258. *Id.* at 179–82.

259. Although the impact of MPCR declines in larger groups, the effect remains positive and significant. *See id.* at 196–97.

260. Chaudhuri, *supra* note 10, at 48–49 ("[C]ontrary to intuition larger groups are no worse—and may even be better—at providing the public good than smaller ones.").

Walker, and fellow economist Arlington Williams confirmed that larger groups could be more efficient than small ones at producing public goods.[261] These results provide a ray of hope for large social networks, or large groups of friends nested within such networks.

Isaac and Walker distinguish between "pure" and "impure" public goods. By "impure" they mean that an increase in group size reduces the marginal benefit from contributing to the public good.[262] For such groups, the increase in size decreases MPCR, thus decreasing cooperation. For pure public goods, increase in size does not decrease MPCR, and therefore does not decrease cooperation. Following this distinction, it may be useful to ask whether privacy is best theorized as a pure or impure public good. Most goods fall somewhere in a range between public and private.[263] Commentators note:

> The in-between points [between purely private and purely public goods] are occupied by impure public goods, whose benefits are partially rival and/or partially excludable. If, therefore, a good does not display both excludability (nonexcludability) and rivalry (nonrivalry) in their pure forms, the good is called impurely public.[264]

Privacy has some attributes of a private good. My own privacy inures both to my private benefit in ways that affect me alone, and my privacy-seeking behavior positively affects others. Privacy can therefore be modeled as impurely public. Likewise, lack of privacy seems to scale nonlinearly with the number of contributors to a system. What a social network knows grows nonlinearly as a function of the number of participants and their contributions. Thus, it seems plausible that the number of participants could impact privacy's social-production function. If this is the case, then the MPCR of privacy-seeking behavior will fall as the number of participants increases. This, in turn, might cause underproduction of privacy.

---

261. *See* R. Mark Isaac, James M. Walker & Arlington W. Williams, *Group Size and the Voluntary Provision of Public Goods*, 54 J. PUB. ECON. 1, 30 (1994) ("Decision-making groups of size 4, 10, 40, and 100 provide replicable results contradicting the widely held premise that a group's ability to provide the optimal level of a pure public good is inversely related to group size.").

262. *See id.*

263. *See* CORNES & SANDLER, *supra* note 3, at 9 ("The literature often treats certain types of physical goods or services as inherently possessing rivalry or nonrivalry, excludability or nonexcludability. However, this can sometimes be dangerous.").

264. *Id.*

On the other end of the spectrum, we can model privacy as approaching a pure public good. One person's consumption of privacy—say, a couple's decision to delay the announcement of a pregnancy—impacts those nearest to them, but may not have much impact on those with whom they do not share a social circle. The switch from primarily impure to approaching pure is likely a fairly rapid falloff once we are discussing the privacy of friends of friends of friends.

From this literature we can draw several insights. First, the MPCR, or, in the case of a public bad, the marginal per-capita loss, within social media may not be high enough to sustain cooperation to avoid accumulating public bads. Isaac and Walker flagged high-number, low-MPCR systems as those most likely to be plagued by efficiency problems. This describes social-media networks and mobile social media fairly directly. In these systems, the losses are so small and nonspecific that users may overcontribute to the system without realizing it. Tiny amounts of damaging data, logged from thousands of different sources, may not incentivize users to avoid loss, in the same way that smaller amounts of per-capita return, when spread across a larger number of players, are less likely to induce efficient contribution to a public good.

To the extent privacy is best modeled as impure, keeping nested groups tight and intimately connected might foster positive cooperation and increase the value of MPCR as a tool for promoting more cooperation. One user's contributions of data impact those close to her much more strongly. Small, tightly nested groups are the best place to leverage MPCR, since the users not only have an effect on each other, but care about the effects they have.[265] The MPCR of privacy in the narrower circle is higher, the connections tighter, and the probability of future cooperation likewise higher. Tools to protect the privacy of friends will help nested groups produce privacy.[266] A good example of useful tools would be controls, already enabled in certain networks, which permit users to differentiate between narrow groups of family and friends, and broader groups of acquaintances. This does, of course, involve a trade-off because users must identify different social circles, but they gain more than they lose by keeping family business in the family.

265. *Id.*

266. *Id.*

To the extent privacy approaches a pure public good—as appears to be the case if one considers the broad run of the Internet without reference to tighter, smaller groups—we are comforted that Isaac, Walker, and Williams posit at least an equal, if not superior, ability to deliver the public good. The experimental evidence provides reason to believe the size of groups, alone, does not disqualify them from cooperating on better privacy outcomes. This has positive policy implications: the further away (not necessarily in a physical sense) someone is from my social network, the less incentive I have to pry into their personal life, and the greater my incentive may be to contribute to systems that protect everyone across the system.

2. *Player Heterogeneity and Conditional Cooperation*. The literature that followed then began to look more closely at group composition in order to find out why some groups can provide public goods and others fail.[267] As one commenter notes, "The most notable [recent] finding in the area is that many participants behave as 'conditional cooperators,' whose contribution to the public good is positively correlated with their beliefs about the contributions to be made by their group members."[268] Conditional cooperators are not altruists. They do not aim at improving others' utility, irrespective of who those others are or what they do. But if a conditional cooperator is sufficiently optimistic that others will resist the temptation to exploit them, they are willing to resist that temptation as well. In the context of online information sharing, conditional cooperation implies that an individual is willing to resist the immediate urge to post some piece of information, and thereby to expose others to informational risk, as long as she is sufficiently optimistic that many others will also be cautious. Thus, *who* one plays with is as important as the rules of the game or the number of players.[269] "This idea that there may be different types of players" was suggested by prior literature, but has only been systematically explored in the last decade.[270]

267. *See* Chaudhuri, *supra* note 10, at 48.

268. *See id.* at 49.

269. *See id*.

270. *See id*. ("We have now come to realize that the usual decaying pattern of contributions can be better understood by appealing to heterogeneity in the types of players interacting with one another.").

The experiments that have identified conditional cooperation test participants in the context of simultaneous one-shot games.[271] In the field, however, many more options are available to a person seeking to determine whether to make private information available online. Even if not within the confines of a group of known others, the individual has had a chance to observe the online platform for a while. In the technical language of behavioral economics, such a person is not forced to rely exclusively on her beliefs, and may update beliefs through her own experiences or those of others, and the individual has little reason to expect others to manipulate her impressions.[272] This is good news. If conditional cooperation is as relevant for information sharing as it is for monetary contributions to experimental public-good games, chances are that the information owners will cooperate to at least mitigate the dilemma. One could expect them to act to mitigate privacy harms as long as they gain the impression that a sufficient fraction of the relevant population will do the same.

The motives that drive conditional cooperation are not yet finally settled. Two explanations have found considerable experimental support: distributional equity ("inequity aversion"),[273] and reciprocity.[274] Inequity aversion exclusively looks at outcomes. A person is inequity averse if she cares not only about absolute profit, but also about relative profit. Inequity-averse individuals do not want to get less than others, and also possibly feel uncomfortable when they get more than others. In the context of online information sharing, inequity aversion could support conditional cooperation if the typical user of the platform in question perceives most other users

271. *See generally* Urs Fischbacher & Simon Gächter, *Social Preferences, Beliefs, and the Dynamics of Free Riding in Public Goods Experiments*, 100 AM. ECON. REV. 541 (2010) (measuring participants' cooperation preferences as well as participants' beliefs about others' contributions); Urs Fischbacher, Simon Gächter & Ernst Fehr, *Are People Conditionally Cooperative? Evidence from a Public Goods Experiment*, 71 ECON. LETTERS 397 (2001) (stating that participants played the game knowing they would not be exposed to the other participants again).

272. For a canonical treatment, see generally Michael Spence, *Job Market Signaling*, 87 Q.J. ECON. 355 (1973).

273. *See* Chaudhuri, *supra* note 10, at 50 (discussing Ernst Fehr & Klaus Schmidt, *A Theory of Fairness, Competition and Cooperation*, 114 Q.J. Econ. 817 (1999); Gary E. Bolton & Axel Ockenfels, *ERC—A Theory of Equity, Reciprocity and Competition*, 90 AM. ECON. REV. 166 (2000)).

274. *See id.* at 50 (discussing Matthew Rabin, *Incorporating Fairness into Game Theory and Economics*, 80 AM. ECON. REV. 1281 (1993); Martin Dufwenberg & Georg Kirchsteiger, *A Theory of Sequential Reciprocity*, 47 GAMES & ECON. BEHAV. 268 (2004)).

to act as she will. If that is the case, by misbehaving herself she exposes others to inequity (in the form of risk or damage) while she reaps the immediate gains from disclosing information. If she is sufficiently averse to doing that, this may suffice to support an environment where little potentially critical information leaks out. Yet the more this individual is skeptical about the behavior of others on that same platform, the more she faces the risk of being herself the one who suffers from their irresponsible behavior. That would lead to disadvantageous inequity. In line with the experimental evidence, models of inequity aversion tend to show that the disutility from being exploited is more pronounced than the disutility from being an exploiter.[275] Yet if the individual is sufficiently optimistic about the behavior of relevant others, the risk of being exploited herself becomes negligible.

The difficulty with inequity aversion is that it may cause groups to coordinate on bad outcomes. If being treated equally is more important to individuals than being treated well (in the absolute sense), groups may choose to coordinate on the easier and worse every-person-for-herself defection outcome in a social dilemma, rather than on the harder and better coordinated outcome that maximizes social welfare. Applying this insight to the privacy context, one is more likely to cooperate in an environment in which each person is perceived to benefit from privacy equally. If privacy protections are perceived to yield unequal benefits, individuals are more likely to defect, especially if they fear being disadvantaged. Inequity aversion may explain the strength of the "nothing-to-hide" fallacy that plagues privacy discussions. The claim does not at first make sense: as Daniel Solove has repeatedly argued, even those with nothing to hide suffer nonzero costs of surveillance.[276] Why then resist privacy rules that benefit both oneself and others? One possible answer suggested by the experimental evidence above is that individuals may assume that bad actors benefit from privacy more

275. *See* Ernst Fehr & Klaus Schmidt, *A Theory of Fairness, Competition and Cooperation*, 114 Q.J. Econ. 817, 822 (1999). For the empirics, see Mariana Blanco, Dirk Engelmann & Hans-Theo Normann, *A Within-Subject Analysis of Other-Regarding Preferences*, 72 GAMES & ECON. BEHAV. 321, 321–37 (2011).

276. *See* Daniel J. Solove, *Why Privacy Matters Even If You Have Nothing to Hide*, CHRON. HIGHER EDUC. (May 15, 2011), https://chronicle.com/article/Why-Privacy-Matters-Even-if/127461 [http://perma.cc/T2TA-J2FB] ("With the disclosure of secrets, the harm is that your concealed information is spread to others. With the peeping Tom, the harm is that you're being watched.").

than other people. Because the bulk of the population consider themselves not to be bad actors, they consider themselves comparatively disadvantaged by such an outcome. It is difficult to find any other reason to resist rules that offer a small benefit to me and a large benefit to someone else. The difference in outcome may generate aversion to producing the benefit.

Leveraging inequity aversion to create privacy will have two components. First, education initiatives could focus on the benefit of privacy to each person and smoothing out perceptions of unequal outcomes in privacy protection. Second, initiatives could help coordinate users on the better equality option of group cooperation, rather than the worse equality option of individual defection. Inequity-averse groups want everyone to be equal—equally well off, or equally harmed. By anchoring expectation on the equal benefits of privacy to all, rather than the dystopian equality of no privacy at all, such initiatives may focus the effect of inequity aversion on generating socially positive outcomes.

Reciprocity, the other explanation for conditional cooperation, focuses on perceived intentions rather than outcomes. If reciprocity is the driving force, conditional cooperation obtains if the individual observes or believes that a sufficient fraction of the relevant others is acting in good faith.[277] We may refuse to participate in the production of public goods because we do not trust others to participate. Conversely, we may be willing to cooperate on the condition that we receive sufficiently strong evidence of others' intent. Thus, "studies have found that players are much more likely to cooperate in a social dilemma when they expect their fellow players to cooperate."[278] Evidence of outcomes may or may not be informative about others' intentions. If the other person's actions directly and predictably caused harm to the conditional cooperator, the cooperator might reasonably infer bad intent. More importantly, if the other person could have acted to cause clear harm, and did not, trust may build, fostering cooperation on group goals. On the other hand, if one were able to prove that a negative outcome was caused by random chance, and not by the bad intent of other group members, a conditional cooperator motivated by reciprocity would continue to be willing to cooperate despite a bad outcome.

---

277. Blair & Stout, *supra* note 42, at 1772 ("Studies have found that players are much more likely to cooperate in a social dilemma when they expect their fellow players to cooperate.").

278. *Id.*

Applied to online privacy, reciprocity theory yields significantly different policy suggestions than does inequity aversion. For example, reciprocity could work to sustain cooperation with respect to correlated information, as with the typical picture in which others feature together with me. In such a case, the outcome provides good information about the intent of the poster. For eBay, Instagram, Facebook, LinkedIn, Twitter, and other channels that permit actions from which intention can be inferred, reciprocity can be expected to play a significant role. But information about intentions is much more difficult to get if the main risk is other people providing grist for better pattern recognition by machine learning algorithms. What is needed is an expression of the positive intentions of others. Advertisements where one actor deletes an embarrassing photo of someone else, or advertising campaigns highlighting steps one can take to protect the privacy of others will help to generate a sense of positive intent on the part of other group members. Testimonials, repeat experience, or reputation-rating systems for friends within narrow social circles can help build a sense of who is trustworthy and who is not.[279] This trust building within social circles cuts against the current approach, which is to promote through schools and advertising that no one can be trusted online. That approach triggers negative views of others' intentions, causing conditional cooperation to fail as each person seeks to protect herself alone. Indeed, the negative view of others' intentions would cause reciprocity-based conditional cooperation to fail even without any experienced negative consequences of others' bad actions.

C. Tools to Resist Social Dilemmas

The tools that foster coordination in groups are different from those needed by individuals to protect their private interests. The economics literature, both experimental and classical, indicate four tools designers can use to increase group coordination: the marginal value of investing in the public good, the ability of members to communicate with one another, the possibility of sending a targeted reaction (often a sanction) to those whose behavior an individual condemns, and changing the light in which individuals view the privacy dilemma. This Subpart addresses each tool in turn.

279. Of course, this remedy itself partly creates a new challenge to privacy, much like a medicine having side effects.

1. *Marginal Per-Capita Return*. As long as the return from individual private investment exceeds the individual marginal payoff from the public good, neoclassical theory would predict that individuals would continue to defect completely regardless of the cooperation or defection of all other players. If neoclassical theory were correct, marginal increases in the payout players receive from contributing to a public good would not positively impact cooperation, until the individual payout for public-good investment exceeded the individual reward for being selfish. In the experimental literature, however, group cooperation is improved significantly by increasing the marginal payoff of contributing.[280] In the lab, cooperation increases as the ratio of payout for investing in a public good rises relative to the level of payout on investments in purely private gain. The effect is confirmed and powerful.[281]

The important policy question for privacy is whether modest incremental increases in the value of privacy-seeking behavior are useful, or whether we must raise the individual payoff of investment in privacy until it exceeds the value of selfish behavior, thus dissolving the social dilemma. The experimental results lead us to believe that increasing the payoff from privacy-seeking behavior, or decreasing the payoff from ignoring the side effects on others' privacy for that matter, will encourage public coordination on better privacy outcomes even if careless behavior remains individually profitable.[282] We do not have to raise the payout from privacy-seeking to a level higher than the individual payout from using privacy-intrusive services.[283] A modest marginal increase in the payoff of privacy-seeking behavior ought to increase the overall amount of privacy society produces.

---

280. *See* Ledyard, *supra* note 10, at 141.

281. *See* Ledyard, *supra* note 10, at 150 (surveying the literature on increased MPCR).

282. *See* Thomas R. Palfrey & Jeffrey E. Prisbrey, *Anomalous Behavior in Public Goods Experiments: How Much and Why?*, 87 AM. ECON. REV. 829, 830 (1997). One of us has shown that the marginal per-capita rate not only has an effect on the level of contributions in a public good, but also on their sustainability. *See* Theodore Eisenberg & Christoph Engel, *Assuring Civil Damages Adequately Deter: A Public Good Experiment*, 11 J. EMPIRICAL LEGAL STUD. 301, 301–49 (2014). Note, however, that the experiment is framed differently. It is concerned with the deterrent effect of an obligation to pay damages, and manipulates the certainty and the severity of this sanction. Yet effectively this translates into a difference of the marginal per-capita rate of contributing to the public good, which increases the expected value of the sanction.

283. *See* Palfrey & Prisbrey, *supra* note 282, at 830.

Law can facilitate such humble increases in payout by providing even limited and incremental increases in the benefit consumers receive from engaging in privacy-seeking behavior. These approaches are often overlooked because they do not completely solve problems, but only provide a little bit of additional benefit. For example, permitting consumers to exercise per-permission control of the information that flows to and from their mobile apps—letting them revoke location-information permissions, or in-app purchase, or phone identity information—would not create comprehensive privacy protection. But it would help a bit. The experimental results lead us to believe that even these modest and incremental improvements can help to encourage positive behavior.

Another practicable way to increase the payout for privacy-seeking behavior is to provide consumers with a method for communicating their expectations and an enforcement mechanism to ensure those expectations are met. For example, one might consider the current dearth of enforcement surrounding consumer-set do-not-track flags.[284] The flag is a feature in every mainstream browser. Consumers must incur time costs to understand and set the do-not-track flag in their browser. Even if they do so, however, companies continue to take the "no" of a consumer as a "yes." Regulatory agencies have not enforced consumers' preferences. As a result, the investment of time by the consumer in understanding and configuring even this most basic privacy technology yields no return. This corrodes consumer willingness to invest in even minimal privacy-seeking behavior. It would be neither legally nor technically complicated to require companies to respect consumers' choices. Doing so would raise the payoff for the consumer's investment in privacy, causing those within the population who are willing to cooperate at this higher payoff to do so. In short, the MPCR literature suggests that small, incremental, and above all politically feasible measures to increase the payout from consumers' privacy-seeking behavior are well worth the candle even if they fall short of making investment in privacy yield benefits greater than self-interested behavior.

284. *See* Fred B. Campbell Jr., *The Slow Death of 'Do-Not-Track'*, N.Y. TIMES (Dec. 26, 2014), http://www.nytimes.com/2014/12/27/opinion/the-slow-death-of-do-not-track.html?_r=0 [http://perma.cc/4W5E-32LB].

2. *Communication*. Because social dilemmas are a coordination problem, communication is a powerful tool to foster group cooperation.[285] Groups that can communicate can coordinate, and those that cannot are severely hampered.[286] As an intuitive matter, therefore, the presence of robust means of communicating between group members ought to be a good way for them to coordinate on the creation of public goods like privacy. However, neoclassical theory predicts that communication will have no impact on a social dilemma. In a dilemma, each player should defect no matter what other players do. This prediction holds regardless of what other players might say about their intentions.[287]

Experiments have again shown some interesting divergence from neoclassical theory. In experiments, permitting participants to identify and communicate with one another increases the provision of public goods.[288] Lifting the veil of complete anonymity powerfully increases cooperation in dilemma situations.[289] Cooperation further increases if individuals have a chance to talk to each other,[290] and if they are given the ability to check and verify whether their fellow participants have followed through on their announced intentions.[291] Cheap, nonbinding talk does not appear to increase contributions. Rather, the effect appears to rely on communication occurring in a setting in which group members can assess the commitment of other players to contributing to the public good.[292] Two broad causes of the effect have been posited from this research: the ability to communicate may promote mutual promises to cooperate, or it may build group identity and cohesion.[293]

---

285. *See* Ledyard, *supra* note 10, at 141.

286. *See* Rick K. Wilson & Jane Sell, *"Liar, Liar . . .": Cheap Talk and Reputation in Repeated Public Goods Settings*, 41 J. CONFLICT RESOL. 695, 697 (1997) [hereinafter Wilson & Sell, *Liar Liar*].

287. *See* Ledyard, *supra* note 10, at 156 ("If there is a unique dominant strategy equilibrium, as is true of most experiments without thresholds, then talking should have no effect on rates of contribution: we should see none.").

288. *See* Ledyard, *supra* note 10, at 156.

289. Bruno S. Frey & Iris Bohnet, *Identification in Democratic Society*, 26 J. SOCIO-ECON. 25, 27 (1997).

290. Gary Charness & Martin Dufwenberg, *Promises and Partnership*, 74 ECONOMETRICA 1579, 1582 (2006).

291. *See* Jane Sell & Rick K. Wilson, *Levels of Information and Contributions to Public Goods*, 70 SOC. FORCES 107, 119 (1991); *see also* Ledyard, *supra* note 10, at 156–57 (surveying studies that have demonstrated how verification improves cooperation).

292. *See* Wilson & Sell, *Liar Liar*, *supra* note 286, at 714.

293. *See id.* at 698.

These results provide both some insight and challenges for the provision of privacy online. It is difficult to imagine a digital privacy scenario in which participants do not have some capacity to communicate. Insofar as communication enables group coordination on welfare-maximizing outcomes, this is positive. On the other hand, the specific public good sought here is privacy. Identifying people and communicating information about them in the name of privacy may at first blush appear contradictory. The key appears to be to provide reliable feedback about the privacy practices of actors when compared to their past promises, not necessarily disclosing further information about the actor's real-world identity. For example, it is not at all common practice for participants in laboratory experiments, even those testing communication, to share real names or other identifying information, yet their ability to communicate during the experiment helps sustain cooperation. Pseudonymity is not merely failed anonymity—pseudonyms permit people to build stable reputations and relationships and communicate with one another while limiting the real-world information they must reveal. For example, an eBay seller can develop a reputation for honest dealing under a pseudonym without revealing her true name, email address, telephone number, or address. Pseudonymous communication permits users to coordinate actions and convey information about past practices without exposing greater amounts of personal information.

3. *Sanction*. Some individuals do not care about others, or they even enjoy seeing them in trouble. Happily, they constitute a minority of those populations that have been rigorously tested.[294] But for those in the population who remain indifferent to the costs of their behavior to others, identification and communication open up the possibility of shaming.[295] Shaming is a social sanction, which is frequently used as a reaction to informational damage. Spread rumors about a sister-in-law, and expect to be ostracized at family gatherings. Air dirty laundry on Facebook, and expect to be defriended.

Such commonsense intuitions are borne out in the public-goods experimental literature. Studies repeatedly show that the availability

294. *See* Joseph Henrich et al., *"Economic Man" in Cross-Cultural Perspective: Behavioral Experiments in 15 Small-Scale Societies*, 28 BEHAV. & BRAIN SCI. 795, 798 (2005).

295. William S. Neilson, *A Theory of Kindness, Reluctance, and Shame for Social Preferences*, 66 GAMES & ECON. BEHAV. 394, 394–403 (2009).

of social sanctions is a very effective technology for securing the provision of a public good.[296] However, sanctions often cost the sanctioning party.[297] Not only does sanctioning activity cost the sanctioning party, it also gives rise to follow-on repercussions. If one person polices the environment, she bears the risk that others might pursue a vendetta against her.[298] Even if one considers the risk of gang up or the costs of imposing sanctions to be small, most people find it unpleasant to assume the role of the cop. In the technical language of welfare economics, vigilance and sanctioning are contributions to a second-order public good.[299] Yet the experimental evidence suggests that, from a policy perspective, one has to be much less concerned about this second-order public good, compared with the original first-order public good. Society can rely on people being upset about others misbehaving, and trying to get them under control.

In principle, this is good news for the protection of privacy. Informal sanction and social ostracism for bad actors is the norm across many online platforms. Features of most platforms support some form of sanction, from defriending to downvoting to shadowbanning, and such sanctions have the additional effect of limiting access to private information by the offender. If I act irresponsibly on a social network, for example, I will be defriended and my access to in-group-only information will be revoked. If I act irresponsibly on a discussion site by revealing the personal details of other posters, I will be banned. Yet sanction depends on repeat play

296. *See, e.g.*, Ernst Fehr & Simon Gächter, *Altruistic Punishment in Humans*, 415 NATURE 137, 137–39 (2002); Ernst Fehr & Simon Gächter, *Cooperation and Punishment in Public Goods Experiments*, 90 AM. ECON. REV. 980, 980 (2000).

297. *See* Martin Sefton, Robert Shupp & James M. Walker, *The Effect of Rewards and Sanctions in Provision of Public Goods*, 45 ECON. INQUIRY 671, 673 (2007).

298. This is not a merely theoretical risk. It even materializes under the controlled conditions of the lab. *See generally* Nikos S. Nikiforakis & Dirk Engelmann, *Altruistic Punishment and the Threat of Feuds*, 78 J. ECON. BEHAV. ORG. 319 (2011) (finding that one-quarter of all punishments are retaliated); Nikos S. Nikiforakis, *Punishment and Counter-Punishment in Public Good Games: Can We Really Govern Ourselves?*, 92 J. PUB. ECON. 91 (2008) (finding that subjects will severely punish their victims in order to deprive their victims of the funds to retaliate).

299. *See generally* Douglas D. Heckathorn, *Collective Action and the Second-Order Free-Rider Problem*, 1 RATIONALITY & SOC'Y 78 (1989) (describing how sanctioning systems manifest in second-level, or intragroup, collective-action problems); Toshio Yamagishi, *The Provision of a Sanctioning System as a Public Good*, 51 J. PERSONALITY & SOC. PSYCHOL. 110, 111 (1986) ("[A]ssuming that people who have developed the goal of mutual cooperation . . . cooperate for the implementation of the needed structural change . . . rather than simply engaging in cooperative actions in the original public good situation . . . .").

and identification, discussed above.[300] In order for a group to impose a sanction, they must know who has defected against group interest, and they must have a mechanism that can deter future defection. Future defection only matters if the member to be sanctioned is a member of a group with the potential to cooperate in the future that can identify and sanction the offender. Mediating the balance between sanction and privacy can be challenging, but good solutions are already in place. Distributed database technology based on trustless public ledgers, such as that used by World Table or other distributed-ledger comment-curating systems, permit users to create persistent pseudonymous identities across multiple platforms—a worldwide online pseudonymous reputation. Once they do, the reputation of the pseudonym can serve as a sanctionable resource. Those with established reputations will be trusted. Those without will not, because they—like eBay sellers with no reputation ranking—will be perceived as attempting to avoid sanction.

4. *Framing*. Mathematically, public goods and public bads are identical.[301] We have found the public-bad story convincing, since in a public-bad game the cooperative decision is not to contribute to the public bad, just as with social media one strong cooperative decision is not to contribute data that bears on or concerns others. Yet it may be that psychologically speaking, conceiving of privacy as a public good could have a salutary effect on attempts to help groups control third-party-generated information online.[302] In a highly cited experiment, James Andreoni demonstrated that framing impacts contributions to a public good, or, conversely, abstention from contributing to a public bad.[303] The pessimistic view of a public bad, or a "cold prickle" as Andreoni described it, seemed to encourage defection.[304] The optimistic view of a public good seemed to engender contribution to the public good, described by Andreoni as a "warm

300. One straightforward way to avoid identification is making negative information about others available in an anonymous way (which presupposes that the victim may not, at least, suspect who has made the information publicly known).

301. *See* Andreoni, *supra* note 9, at 5.

302. *See* Hartzog & Stutzman, *supra* note 128, at 417.

303. *See* Andreoni, *supra* note 9, at 2.

304. *See id.* at 13 ("[W]hen the positive externality is rephrased to be presented as a negative externality—even though the incentives do not change—the provision of the public good . . . [collapses] after ten iterations . . . .").

glow."[305] In short, even though the decision to contribute private information that impacts others may be most accurately described as a public bad, it may perhaps be usefully described to groups seeking to avoid the negative effects of this bad as a public good. In discussing the problem with the public, it may well be better to encourage social-network participants to protect the privacy of other members of their social network than to avoid contributing to the pools of data that can have toxic effects on those members. The one construction may create a warm glow, while the other yields only a cold prickle.

The economic literature refers to such interventions as "valence framing": the structure of the interaction, or its payoffs, are represented in some alternative form. An even more subtle intervention is called "label framing."[306] Some cue evokes some context that, one has reason to believe, will change how individuals act. For instance, it has been shown that experimental participants are much more likely to cooperate in a dilemma game if this game is called a "community game," rather than a "Wall Street game."[307] Likewise, participants cooperate more if the situation is described as a "joint project" or "jointly protecting against danger," rather than "competition."[308]

Given this, it matters more than ever how society talks about privacy. If those seeking to jointly protect themselves against commercial and government exploiters of data do face a public-goods problem, as this Article has sought to demonstrate, it may help to name it as such. Too few seem to see their information-sharing behavior in that light. The experimental evidence suggests that it might be helpful just to let them know. Merely encouraging people to contribute to the public good of privacy may drive up investment in privacy-protecting behavior.

Conversely, if society continues to debate privacy in purely individualistic terms, as it has largely done until this point, the

---

305. *See id*. ("People are significantly more willing to cooperate in a public goods experiment when the problem is posed as a positive externality rather than as a negative externality.").

306. *See* Martin Dufwenberg, Simon Gächter & Heike Hennig-Schmidt, *The Framing of Games and the Psychology of Play*, 73 GAMES & ECON. BEHAV. 459, 461–62 (2011).

307. *See* Lee Ross & Andrew Ward, *Naive Realism in Everyday Life: Implications for Social Conflict and Misunderstanding*, *in* VALUES AND KNOWLEDGE 103, 106–08 (Edward S. Reed, Elliot Turiel & Terrance Brown eds., 1996).

308. Christoph Engel & David Rand, *What Does "Clean" Really Mean? The Implicit Framing of Decontextualized Experiments*, 122 ECON. LETTERS 386, 387 (2014).

experimental evidence indicates that the individual focus will lead to underprovision of privacy. An "every-person-for-herself" mentality will predominate, reducing cooperative behavior. Worse, as individuals fail in the face of the social dilemma, they will be individually blamed. Under the individual privacy narrative, people who do not benefit from privacy must not be trying hard enough, or must not value privacy after all. This Article has taken an initial step toward countering this narrative, by naming the dilemma of privacy for what it is, and by encouraging a positive framing for a longstanding conundrum of social interaction: privacy is a public good.

CONCLUSION

There is some ground for optimism in the otherwise grim field of data privacy. The current dominant approach of focusing on individual education and empowerment has fallen short. This has led to the strange rise of privacy nihilism, that is, the claim that since consumers cannot get privacy, they must not want it. The focus on individual empowerment underemphasizes the group or community dimension of privacy.

The focus on empowering individuals has induced policymakers to overlook important tools for protecting privacy. The relevant privacy unit is the group, rather than the individual. Social dilemmas pit individuals against each other, and individual incentives cut against group welfare. In many ways, the more educated and empowered individuals are, the worse the social dilemma becomes for the group.

Features of the privacy debate function in ways that are similar to a social dilemma. The well-known public-good (public-bad) dilemma best matches the contours of the privacy debate. It does not exclude other models. We merely claim that individual-focused approaches have reached diminishing returns, and that approaches focused on groups may yield more fruit for the investment. The public-goods model has a broad range of tools suggested by the theoretical and experimental economic literatures that have gone underexplored thus far in the privacy debate.

In exploring these tools, we note a debate internal to the economics literature that has important ramifications for the study of privacy. Classical economic theory predicts that many tools groups use to increase cooperation should have no effect: in the face of a

social dilemma, all cooperation should collapse. Experimentalists have on the other hand consistently confirmed that groups resist social dilemmas to the benefit of the group and to individual members' detriment, and that certain tools help. Whether this resistance to social dilemmas is learned and becomes a heuristic over a lifetime of confronting such situations, or whether humans innately struggle against social dilemmas, we take this struggle as a sign of hope.

This Article proposes giving groups tools for this struggle. Policymakers should consider the size, composition, and cohesion of online groups when they attempt to create an environment conducive to privacy protection. Tools should not be centered on individual rights of review and deletion, which have proven largely ineffective. Rather, tools should focus on group communication, sanction, and fostering a sense of repeat play and community. Even the way that we speak about the nature of the problem can have an impact on whether people cooperate to produce the public good of privacy.

The highest aspiration of an academic article is not to settle a debate, but to spur further inquiry. We do not claim to have identified the best solutions from a legal policy perspective, and we believe that much fruitful behavioral-economic research is yet to come. We hope, however, that the door is now open, and that the overindividualized approach to privacy protection will yield to a more balanced debate about the tensions between individuals and groups in the privacy context.