2015

Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements

A. Michael Froomkin
University of Miami School of Law, froomkin@law.miami.edu

REGULATING MASS SURVEILLANCE AS PRIVACY POLLUTION: LEARNING FROM ENVIRONMENTAL IMPACT STATEMENTS

*A. Michael Froomkin**

Encroachments on privacy through mass surveillance greatly resemble the pollution crisis in that they can be understood as imposing an externality on the surveilled. This Article argues that this resemblance also suggests a solution: requiring those conducting mass surveillance in and through public spaces to disclose their plans publicly via an updated form of environmental impact statement, thus requiring an impact analysis and triggering a more informed public conversation about privacy. The Article first explains how mass surveillance is polluting public privacy and surveys the limited and inadequate doctrinal tools available to respond to mass surveillance technologies. Then, it provides a quick summary of the Privacy Impact Notices ("PINs") proposal to make a case in principle for the utility and validity of PINs. Next, the Article explains how environmental law responded to a similar set problems (taking the form of physical harms to the environment) with the National Environmental Policy Act of

* Laurie Silvers & Mitchell Rubenstein Distinguished Professor of Law, University of Miami.

Invaluable research assistance was provided by U. Miami Law Reference/Faculty Services Librarian Barbara Brandon. Thanks for helpful comments to Caroline Bradley (multiply) and for comments and conversations to Jonathan Baker, Jane Bambauer, Caroline Corbin, Mary Anne Franks, Bob Gellman, Steve Gold, Patrick Gudridge, Lynn Goldstein, Dennis Hirsch, Seth Kreimer, Jessica Litman, Felix Mormann, Leigh Osofsky, Charles Raab, Peggy Radin, Michael Ravnitzky, Peter Swire, Lee Tien, Steve Vladeck, Jonathan Weinberg, Richard Williamson, and Jonathan Zittrain. I also benefited significantly from comments on earlier drafts by participants in the University of Pennsylvania's Center for Technology, Innovation and Competition Workshop, Fordham Law School's Center for Information Law & Policy Faculty Workshop, American University Washington College of Law's Faculty Workshop, the University of Miami School of Law Internal Speaker Series, and the 2013 Privacy Scholars Conference. I am particularly grateful to Steven E. Koonin for sharing his slides from his stimulating – and, frankly, terrifying – talk about CUSP at the Simons Foundation in March, 2013 which inspired this article, and also for providing additional information about CUSP's plans and for commenting on an early draft. All remaining errors are entirely my own.
I should disclose that I serve on the Advisory Boards of two organizations mentioned in this article: the Electronic Frontier Foundation and the Electronic Privacy Information Center, and am a non-resident fellow of a third, the Center for Democracy and Technology.

1969 ("NEPA"), requiring Environmental Impact Statement ("EIS") requirements for environmentally sensitive projects. Given the limitations of the current federal privacy impact analysis requirement, the Article offers an initial sketch of what a PIN proposal would cover and its application to classic public spaces, as well as virtual spaces such as Facebook and Twitter. The Article also proposes that PINs apply to private and public data collection—including the NSA's surveillance of communications. By recasting privacy harms as a form of pollution and invoking a familiar (if not entirely uncontroversial) domestic regulatory solution either directly or by analogy, the PINs proposal seeks to present a domesticated form of regulation with the potential to ignite a regulatory dynamic by collecting information about the privacy costs of previously unregulated activities that should, in the end, lead to significant results without running afoul of potential U.S. constitutional limits that may constrain data retention and use policies. Finally, the Article addresses three counter-arguments focusing on the First Amendment right to data collection, the inadequacy of EISs, and the supposed worthlessness of notice-based regimes.

TABLE OF CONTENTS

I. INTRODUCTION

Personal privacy in developed countries is disappearing as quickly as the polar ice caps. The rapid growth in the number and breadth of databases, the continuing drop in the costs of information processing, the spread of cheap sensors, and the rise of self-identification practices, have all combined to make this the era of Big Data. Much like global warming, drift-net data collection and collation creates widespread harms substantially caused by actions not visible to most of those affected. Both the private sector and the government find value in collecting vast amounts of information about everyone: firms collect personal data for marketing and revenue maximization; governments collect personal data for everything from efficiency to security. Practically nothing and nowhere is exempt: data are collected in the home, from cell phones, online, and in public spaces. Market failures, collective action problems, and especially information asymmetries—including, we have recently learned, a stunning lack of government transparency about domestic surveillance—characterize the current privacy crisis, much as they did the environmental problem in the 1960s.

Encroachments on privacy, and especially on privacy in public,[1] greatly resemble the pollution crisis in that they impose externalities on others. Our initial response to the original pollution crisis provides a possible initial solution to this new form of pollution of both the public and private spheres: requiring those proposing to watch us in and through public spaces to disclose their plans publicly via an updated form of environmental impact statement that will help protect everyone's privacy. Mandating full disclosure will require those imposing mass surveillance on others to do an impact analysis; if they do not do it well they may be subject to suit and their projects may be delayed. This incentive to re-

1. For thoughtful early work on the value of and threats to privacy in public, see Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004); Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 J. L. & PHIL. 559 (1998); Helen Nissenbaum, *Toward an Approach to Privacy in Public: The Challenges of Information Technology*, 7 J. ETHICS & BEHAV. 207 (1997).

search the consequences of mass surveillance will prime an informed conversation about privacy in public. Additionally, the need to build in consideration of the consequences of surveillance into project planning, as well as the risk of bad publicity arising from excessive surveillance proposals, will act as a counterweight to the adoption of mass data collection projects, just as it did in the environmental context. In the long run, well-crafted disclosure and analysis rules could pave the way for more systematic protection for privacy—as it did in the environmental context. At present, we know relatively little about how to measure the costs and benefits of personal information acquisition and uses. In order to make the case for substantive regulation of privacy-harming practices in the United States, we will need to know a great deal more about who is being watched and what is being collected. The privacy equivalent of the environmental impact statement will tell us much, and will also provide occasions to grow expertise about privacy harms and mitigation strategies.

Environmental impact statements may be out of fashion today, but they played an important role in educating the public, policy-makers, and also builders, about environmental risks and costs, especially in the early days of environmental regulation. In the United States, these are still the early days of privacy regulation. We can apply what we have learned from more than thirty years of environmental disclosures to craft a better regime for disclosure, and thus analysis and debate, of the rapidly increasing number of public and private projects that involve mass surveillance. By providing well-crafted safe harbors for legitimate projects we can also ensure that the disclosure requirement does not become a hurdle to many meritorious projects, and restrict the number and scope of projects that might become subject to lawsuits alleging insufficient disclosure.

Part II of this Article explains how mass surveillance is polluting our privacy, giving examples of mass surveillance activities drawn from the private and public sectors. It argues that mass surveillance is already very great, is growing, and that it is difficult to monitor and poorly understood. This Part also discusses how the deployment of potentially privacy-harming technology can be seen as a form of market failure. Having shown that we face a large problem, Part II then demonstrates that existing doctrinal legal tools are inadequate to respond to the deployment of mass surveillance technologies, and especially when it comes to surveillance in or through public spaces. Then it provides a very quick summary of the Privacy Impact Notices ("PINs") proposal, noting that the aim of this Article is to make the case in principle for the utility and validity of PINs without tying the argument to any particular level of coverage. Level of coverage could vary, ranging from a very tame, and thus less useful, requirement that applied only to government-sponsored, non-intelligence projects to a much more sweeping coverage that extended to large-scale private data collection activities in physical space and online.

Of these, the most controversial elements would undoubtedly be whether to cover the vast data-gathering of entities such as the NSA, and whether to impose a requirement that private firms planning vast data-gathering first disclose it and be subject to suit if they fail do so fully and accurately.

Part III then explains how, with the National Environmental Policy Act of 1969 ("NEPA"),[2] environmental law responded to a similar set of market failure problems relating to physical harms to the environment. It outlines the main features of the Environmental Impact Statement ("EIS") requirement for environmentally sensitive projects and then argues that we can learn from NEPA's successes and defects in order to craft a PIN requirement triggered by plans to engage in mass surveillance. It contrasts the PIN proposal to the existing, much more limited, federal privacy analysis requirement, known as Privacy Impact Assessments. Part III also provides an initial sketch of what a PIN proposal would cover, in particular which sorts of activities would have presumptive safe harbors and which would likely be subject to the most thorough analysis and disclosure requirements. As with NEPA, incomplete disclosures of the scope of surveillance or its likely effect on privacy could give rise to lawsuits. The final section of Part III examines whether the PIN proposal would have applications to surveillance and data-collection in online public spaces such as Facebook, Twitter, and other virtual spaces. It also considers what the PIN proposal would have to offer towards addressing the now-notorious problem of the NSA's drift-net surveillance of telephone conversations, emails, and web-based communications.

Part IV offers a defense of the PIN proposal against three likely counter-arguments: the claim that there is a First Amendment right to data collection, the claim that EISs are a poor policy tool not worthy of emulation, and the claim that notice-based regimes are in general worthless.

Lastly, Part V provides a brief summary and conclusion.

II. HOW SURVEILLANCE IS POLLUTING OUR PRIVACY

Privacy[3] is an essential political, social, economic, and psychological shield. Information is power; conversely, privacy—the withholding of information—enhances freedom from those who would exercise that power. This rule applies to politics and public administration, as governments

2. National Environmental Policy Act of 1969, 42 U.S.C. §§ 4321–4335 (2012).

3. In what follows, I will treat "privacy" as the ability to control the release of information about oneself. That is certainly not the only possible definition, and it may be incomplete, but it is an approach with a distinguished pedigree, *e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM x (1967), it covers a substantial amount of the territory, and it suffices for these purposes. One might alternately treat privacy as a public good, much like environmental quality. In this lens, privacy has value to an individual not only because it protects disclosure of facts about oneself, but because it shields one from exposure to unwanted facts about others. An economist might retort that if information is valuable, having more of it will always be desirable. And yet, people commonly speak of having "too much information" about another.

can use information to hand out benefits and to select people for punishments.[4] The rule applies in the private sector, where information determines everything from employment and credit to targeting for advertising and discounts. It applies in the personal sphere, where information determines reputations and informs social relations; here, privacy provides room for personal experimentation and provides the space to change. Not least, privacy serves as a critical psychological shield, creating a space for freedom to read, to talk, to think, and sometimes to act, or to experiment.[5] Like most good things, too much privacy can be abused, as when secrecy becomes conspiracy or when the hiding of key information can become part of crime or fraud. But a world without privacy, a world of ubiquitous monitoring and a permanent, indelible, accessible record, would be one of highly chilled speech and very limited freedom.[6]

In light of privacy's relevance to most facets of our lives, it is not surprising that Americans believe their personal information is, or should be, private.[7] Despite this, it is often said that people in developed countries do not care much about privacy.[8] They may tell pollsters that they care, the argument goes, but the revealed preferences of consumers, of voters, and—to whatever extent it actually reflects the popular will—of their elected representatives, all suggest that privacy is frequently a distant second to other values such as lower price (free online content![9]), convenience, security, and fifteen seconds of fame (Twitter, Facebook, webcams). Americans, it is argued, "will sell their privacy for [a] frequent flyer mile."[10] In fact, while privacy-enhancing features are important to

4. Protection from surveillance becomes particularly necessary when the targets have unorthodox political beliefs, especially when the government acts "under so vague a concept as . . . 'domestic security.'" United States v. U.S. Dist. Court for the E. Dist. of Mich., S. Div. (Keith), 407 U.S. 297, 314 (1972); *cf.* Seth F. Kreimer, *Watching the Watchers: Surveillance, Transparency, and Political Freedom in the War on Terror*, 7 J. CONST. L. 133, 149 (2004).

5. In *Bartnicki v. Vopper*, both the majority and the dissent agreed that "privacy of communication is essential if [democratic] citizens are to think and act creatively and constructively" because fear of being monitored can inhibit the willingness to voice critical ideas. 532 U.S. 514, 533 (2001) (citation and internal quotation marks omitted); *id.* at 543 (Rehnquist, C.J., dissenting) (citation and internal quotation marks omitted). A similar argument can surely be made for freedom of association, movement, or reading habits, as well as many other activities. *Cf.* Margot Kaminsky & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465 (2015).

6. *See, e.g.*, Thornburg v. Am. Coll. of Obstetricians & Gynecologists, 476 U.S. 747, 767 (1986) (noting "reporting requirements [would] raise the specter of public exposure and harassment of women" choosing to exercise their right to terminate a pregnancy); Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87, 98 (1982) (noting "risk of harassment" to contributors if exposed).

7. *See* Jennifer M. Urban et al., *Mobile Phones and Privacy* (UC Berkeley Public Law Research Paper No. 2103405, 2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405 (finding "[t]hat Americans overwhelmingly consider information stored on their mobile phones to be private—at least as private as information stored on their home computers").

8. *See, e.g.*, A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1502 (2000).

9. As regards a taste for privacy, younger people differ from older ones primarily in that they are more willing to exchange personal data for free online content or services. *See* Jay Stanley, *Do Young People Care About Privacy?*, ACLU BLOG (Apr. 29, 2013, 10:00 AM), http://www.aclu.org/blog/technology-and-liberty/do-young-people-care-about-privacy.

10. *See* Froomkin, *supra* note 8, at 1502.

consumers and universally appreciated, there appears to be no systematic association between a consumer's level of concern for privacy issues and her privacy choices.[11] A user's level of technological experience, however, positively correlates with her willingness to pay for privacy-enhancing features.[12]

The disjunction between the privacy that people say they want, and the privacy that they actually get is more acute today than ever before, in substantial part due to the poorly understood consequences of their technological choices.[13] This is particularly clear when one focuses on "information privacy" (defined as "the ability to control the acquisition or release of information about oneself"[14]). Potentially privacy-harming technologies are growing by leaps and bounds. Fifteen years ago, the catalog of the worst looming threats to privacy ranged from license plate monitoring to "smart dust"—"ubiquitous miniature sensors floating around in the air."[15] Today, however, new and different potentially privacy-harming projects—operating at a scale undreamed of at the turn of the century—are in deployment, or in advanced stages of preparation.

A. Ubiquitous Sensors

The cost of sensors and information processing is shrinking very quickly. We not only have Moore's law for computing, but a very rapid decrease in the cost of sensors.[16] Cameras are already ubiquitous in major cities; they are being supplemented with devices that detect noise, heat, and the entire spectrum of light.[17] In addition, public and private actors are increasingly tracking cell phones in order to accumulate either aggregate or individual data about personal movements.[18] Public bodies from

11. Sören Preibusch, The Value of Privacy in Web Search 1 (Microsoft Research Cambridge, The Twelfth Workshop on the Economics of Information Security, June 2013) (unpublished manuscript), *available at* http://preibusch.de/.

12. Scott J. Savage & Donald M. Waldman, The Value of Online Privacy 29–30 (Univ. of Colo. at Boulder, Working Paper No. 13-02, 2013). Consumers are much more willing to incur privacy intrusions in exchange for receiving a payment than they are to pay to be free from privacy intrusions. Alessandro Acquisti et al., *What Is Privacy Worth?*, 42 J. LEGAL STUD. 249, 267–68 (2013). Similarly, consumers have a tendency to be content with the level of privacy with which they are currently endowed, regardless of the protection afforded. *Id.* at 264.

13. *See generally* Froomkin, *supra* note 8.

14. *Id.* at 1463.

15. *Id.* at 1500. Smart dust is still on the drawing board, with applications ranging from monitoring our movements to monitoring our insides. *See* Quentin Hardy, *Big Data in Your Blood*, N.Y. TIMES, Sept. 7, 2012, http://bits.blogs.nytimes.com/2012/09/07/big-data-in-your-blood/; John D. Sutter, *'Smart Dust' Aims to Monitor Everything*, CNN (May 3, 2010, 8:27AM), http://www.cnn.com/2010/TECH/05/03/smart.dust.sensors/index.html.

16. DISTRIBUTED SENSOR NETWORKS 31 (S. Sitharama Iyengar & Richard R. Brooks eds., 2005); Teena Hammond, *Looks Are Everything in Wearable Tech*, TECHREPUBLIC (July 29, 2014, 1:17 PM), http://www.techrepublic.com/article/looks-are-everything-in-wearable-tech/.

17. Gerhard P. Hancke et al., *The Role of Advanced Sensing in Smart Cities*, 2013 SENSORS 393, 416–17 (2013); *The Recorded World, Every Step You Take*, ECONOMIST, Nov. 16, 2013, http://www.economist.com/news/leaders/21589862-cameras-become-ubiquitous-and-able-identify-people-more-safeguards-privacy-will-be.

18. *See* Robert X. Cringely, *They Know Who You Called Last Summer*, INFOWORLD (July 09, 2012), https://www.infoworld.com/t/cringely/they-know-who-you-called-last-summer-197274 ("U.S.

toll collectors to police departments collect data about cars by tracking vehicle license plates[19] or transponders. Meanwhile, a whole new generation of biometric sensors is becoming available.[20] Both people and objects can be tracked in surprising detail.

Tracking is attractive because it promises security and riches. The security rationale for surveillance is exemplified by popular reaction to the May 2013 bombing of the Boston Marathon. Three days after the bombing, the FBI released photos of the leading suspects and appealed successfully to the public to identify them.[21]

Tracking also seems to promise outcomes that lead to private profit and public efficiencies. Location tracking has for some time been thought to permit location-based marketing as well as more detailed collection of information about consumers' shopping and other habits.[22] For example, mapping commuting patterns allows cities to better design bus routes and holds out the promise of real-time adjustments based on demand.[23] More generally, and as discussed further below, urban planners and others hope to optimize service delivery—and rule enforcement.

Below, I offer two illustrative examples of projects designed to harness the power of sensors. They make, I submit, an excellent case for the need for the notice-based regime proposed in this Article. These examples are truly illustrative. I could at least as easily have selected other local,[24] state,[25] or national[26] examples. When it comes to information collec-

---

law enforcement agencies requested data from wireless carriers more than 1.3 million times last year.").

19. *See* Cyrus Farivar, *Your Car, Tracked: The Rapid Rise of License Plate Readers*, ARSTECHNICA (Sept. 27, 2012, 8:30 PM), http://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers/; *see also* Jennifer Lynch & Peter Bibring, *Automated License Plate Readers Threaten Our Privacy*, ELEC. FRONTIER FOUND. (May 6, 2013), https://www.eff.org/deeplinks/2013/05/alpr.

20. *See* Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475, 1476 (2013) ("[E]xplor[ing] the constitutional and other legal consequences of big data cybersurveillance generally and mass biometric dataveillance in particular.").

21. *See* Matt Smith & Thom Patterson, *FBI: Help Us ID Boston Bomb Suspects*, CNN (Apr. 19, 2013, 5:44 AM), http://www.cnn.com/2013/04/18/us/boston-blasts. As it happens, one of the highest resolution photos was from a private iPhone, not a security camera. Ravi Somaiya & Jeremy Zilar, *New, Higher-Resolution Image of Boston Marathon Suspect Emerges*, THE LEDE (Apr. 18, 2013, 11:13 PM), http://thelede.blogs.nytimes.com/2013/04/18/new-higher-resolution-image-of-boston-marathon-suspect-emerges/.

22. *See* Froomkin, *supra* note 8, at 1475–76.

23. *See* David Talbot, *African Bus Routes Redrawn Using Cell-Phone Data*, MIT TECH. REV. (Apr. 30, 2013), http://www.technologyreview.com/news/514211/african-bus-routes-redrawn-using-cell-phone-data/ (Reporting that "[r]esearchers at IBM, using movement data collected from millions of cell-phone users in Ivory Coast in West Africa, have developed a new model for optimizing an urban transportation system."). Also, "if the data were available in real-time—rather than months after it was created—the results could be even more powerful. This would provide snapshots of people moving around in a city, allowing the optimal shifting of routes, and reducing travel and wait times. . . ." *Id.*

24. *E.g.*, ACLU, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS, 12–13, 21 (July 17, 2013), *available at* https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf (noting millions of license plate records being collected and retained indefinitely across USA).

25. *E.g.*, The California Smart Grid Initiative; *see* Jennifer M. Urban, *Privacy Issues in Smart Grid Deployment* (Draft 2012 on file with author); *see also* John R. Forbush, Note, *Regulating the Use and Sharing of Energy Consumption Data: Assessing California's SB 1476 Smart Meter Privacy Statute*,

tion, traditional distinctions between public and private often become particularly arbitrary. Private entities that collect data are in almost every case only too happy to sell it to government agencies; even if they will not sell it, that data remains subject to collection and (as we have recently learned) monitoring. Conversely, cash-strapped governments often want to monetize their assets, and because data is non-rivalrous, governments can sell it but still keep it—something one cannot do with most real or tangible assets.

1. Watching the City: State Action

The New York Police Department ("NYPD") has, together with Microsoft, deployed the Domain Awareness System ("DAS"), an extensive monitoring system designed to monitor New Yorkers.[27] The DAS incorporates more than 3,500 cameras in public spaces, license-plate readers, radiation detectors, real-time alerts transmitted from the 911 emergency system, and Police Department data including arrests and parking summonses.[28] Microsoft officials said they have actively negotiated with a number of prospective buyers.[29] Similar systems are in use at home—for example Dayton, Ohio relies on plane-mounted cameras for city surveillance[30]—and abroad.[31]

Creating a database recording everyone's movements allows the state to learn who associates with whom. It chills the freedom of association no less than requiring organizations to publish their membership lists.[32] A government that has access to 24/7 information about the movements and habits of people is one that, even when acting within the law, has the power to investigate people for their political activities.[33] If a

---

75 ALB. L. REV. 341 (2012). California's new law allows data collection, but requires opt-in consent before the data can be shared with third parties. *Id.* at 343.

26. *See, e.g.*, Bureau of Alcohol, Tobacco & Firearms, Investigative System, *R—OPTION - Investigative System*, FEDBIZOPPS.GOV (Aug. 21, 2013, 8:31 AM), https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=8c9638f5b657a484b0a6336558183251&_cview=0.

27. Sam Roberts, *Police Surveillance May Earn Money for City*, N.Y. TIMES, Apr. 3, 2013, https://www.nytimes.com/2013/04/04/nyregion/new-york-citys-police-surveillance-technology-could-bring-in-money.html.

28. *Id.*

29. *Id.*

30. Cyrus Farivar, *The Airborne Panopticon: How Plane-mounted Cameras Watch Entire Cities*, ARS TECHNICA (July 10, 2014, 4:12 PM), http://arstechnica.com/tech-policy/2014/07/a-tivo-for-crime-how-always-recording-airborne-cameras-watch-entire-cities/.

31. *See, e.g.*, RAAB ET AL., INFORMATION COMMISSIONER'S REPORT TO PARLIAMENT ON THE STATE OF SURVEILLANCE, INFO. COMMISSIONER'S OFF (Nov. 2010), *available at* https://ico.org.uk/media/about-the-ico/documents/1042386/surveillance-report-for-home-select-committee.pdf (describing extensive use of ANPR in UK).

32. *See* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 466 (1958) (holding that constitutional rights of speech and assembly include a right of private group association).

33. *See, e.g.*, Matt Sledge, *Homeland Security Tracked Occupy Wall Street 'Peaceful Activist Demonstrations,'* HUFFINGTON POST (Apr. 3, 2013, 9:31 AM), http://www.huffingtonpost.com/2013/04/02/homeland-security-occupy-wall-street_n_3002445.html; *see also* Handschu v. Special Servs. Div., 273 F. Supp. 2d 327, 338 (S.D.N.Y. 2003) (approving an order modifying consent decree to permit additional political surveillance by NY police due to "fundamental changes in the threats to public security" caused by terrorism).

government, or a government official, is less concerned with legal punctilio, the opportunities for abusing that information are greater still.[34] Even Amitai Etzioni, very much a middle-of-the-road commentator on privacy matters, described the DAS—which he nicknamed "Big Eye"—as capturing so much information that even with its built-in legal and technological constraints, it subjects the public to an invasion of privacy "much greater than anything we have seen so far."[35] New York is not only surveilling its citizens, it has an enthusiastic marketing campaign for the surveillance software and hopes to make millions of dollars selling it to domestic and foreign customers.[36]

2. *Watching the City: 'Private' Action*

Regarding potentially privacy-harming technologies, the public/private distinction is of less relevance than one would expect because budgets are the only significant constraint on the government's acquisition of information collected by formally "private" actors. Conversely, governments increasingly see the personal data they collect as an asset ready to be monetized. Data thus moves between the public and private sectors with relative ease,[37] and that ease can only be expected to increase as the cost of data-acquisition drops.

Thus, the threat to privacy from private watchers is substantial, and perhaps as great as the threat from state surveillance. Private actors are not subject to key constitutional and statutory limitations we impose upon our government. Neither the First nor the Fourth Amendment constrain private actors,[38] so long as the state avoids turning them into state actors (and absent the private actor committing a tort or a crime), the

34. Consider the FBI's constant surveillance of Martin Luther King, and J. Edgar Hoover's attempts to use the results of that surveillance to either blackmail Dr. King or perhaps to drive him to suicide. *See* Jen Christensen, *FBI Tracked King's Every Move*, CNN (Dec. 29, 2008, 1:43 PM), http://www.cnn.com/2008/US/03/31/mlk.fbi.conspiracy/.

35. Amitai Etzioni, *The Big Eye Is Not in the Sky*, HUFFINGTON POST (Jan. 23, 2013, 12:45 PM), http://www.huffingtonpost.com/amitai-etzioni/the-big-eye-is-not-in-the_b_2534915.html.

36. *See* Roberts, *supra* note 27.

37. There are some important exceptions to this generalization. Voter rolls are considered public documents not suited for profit-seeking. *See* Ira Rubinstein, *Voter Privacy in the Age of Big Data*, 5 WIS. L. REV. 861, 870 (2014). Some government records are provided at nominal fees that are supposed to reflect the cost of copying. Census records are supposed to be released only in sufficiently aggregated form such that individual entries are not discernable. *But see* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1718, 1756 (2010). A few statutes protect specific mandatory databases. Individual tax information is not released. *See* 26 U.S.C. § 6103 et seq. (2012). Enacted in response to an outcry about states' sales of driver's license photos and registration information, Congress enacted the Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 et seq. (2012), which protects motorist photos and other license information from disclosure (i.e. sale) without the motorist's consent. *Cf.* Reno v. Condon, 528 U.S. 141, 143 (2000) (upholding DPPA against constitutional challenge).

38. United States v. Jacobsen, 466 U.S. 109, 130 (1984) ("[T]he Fourth Amendment is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual") (internal citations & quotations omitted); Gitlow v. New York, 268 U.S. 652 (1925) (reading the Fourteenth Amendment to apply the First Amendment to states as well as the federal government).

private watchers are able to collect data in ways not available to the state directly.

Mass surveillance by private collection of data is not necessarily easy to see. Except when it is contractual, such as a cell phone app provider's monitoring of cell phone use or contact lists, there may be no duty to disclose the fact of the monitoring itself nor the sale or exchange of the data. This forces us to extrapolate somewhat from the acts of bodies that must be, or have chosen to be, relatively public about their plans and capabilities. One such body is NYU's Center for Urban Science and Progress ("CUSP"). CUSP opened shop in Brooklyn in April 2012.[39] It brings together a large group of scholars, projected to grow up to thirty faculty and twenty senior researchers drawn from industrial partners, assisted by an army of postdocs, doctoral candidates, and Masters students.[40] Together they will attempt to create a giant database about what goes on in New York City.[41] Because it is part of a United States university, CUSP's ability to collect personally identifiable data about individuals without their consent is limited by its need to pre-clear that data collection and its use with an internal institutional review body designed to regulate research on human subjects.[42] Although these institutional constraints could prevent CUSP itself from creating a giant database about the activities of most if not all New Yorkers, the technologies CUSP intends to use gives us a window into what would be possible in other, less constrained, private hands.[43]

City-monitoring technologies could, in the not-too-distant future, include data about nearly every person, building, and vehicle in a city. Designers of these initiatives have ambitions that range from measuring noise pollution, collecting every loud sound in the city, to gauging residents' movement patterns, nutrition, energy usage, and even their opin-

---

39. *How and Why CUSP Came to Be*, CENTER FOR URB. SCI. & PROGRESS, http://cusp.nyu.edu/about-how/ (last visited Aug. 8, 2015).

40. STEVEN E. KOONIN, CENTER FOR URB. SCI.& PROGRESS, THE PROMISE OF URBAN INFORMATICS 9 (May 30, 2013), *available at* http://cusp.nyu.edu/wp-content/uploads/2013/07/CUSP-overview-May-30-2013.pdf [hereinafter CUSP Promise].

41. *Id.* at 8.

42. *Id.* at 18–19; *see also* LYNN A. GOLDSTEIN, CENTER FOR URB. SCI. & PROGRESS, EXAMPLE OF BIG DATA IN ACTION WITH CONTROLS: BIG DATA AND CITY LIVING 22 (Dec. 4, 2014), *available at* http://informationaccountability.org/wp-content/uploads/Example-of-Big-Data-in-Action-with-Controls-Big-Data-and-City-Living-Updated.pdf.

43. CUSP is legally private, being run by NYU, a private university. Nevertheless, by design CUSP enjoys a "special relationship" with many government agencies. CUSP Promise, *supra* note 40, at 14. CUSP operates with the support and encouragement of the New York City Applied Sciences Initiative. New York City is expected to be one of the major 'customers' of CUSPs databases. Steven E. Koonin, *The Promise of Urban Informatics (Video)*, CENTER FOR URB. SCI. & PROGRESS at 0:33 (Aug. 2, 2013), http://cusp.nyu.edu/the-promise-of-urban-informatics-video/ [hereinafter Koonin Presentation]; *see also* Steve Lohr, *SimCity, for Real: Measuring an Untidy Metropolis*, N.Y. TIMES Feb. 23, 2013, http://www.nytimes.com/2013/02/24/technology/nyu-center-develops-a-science-of-cities.html. CUSP receives New York City and corporate funding, and lists four Department of Energy National Laboratories. CUSP Promise, *supra* note 40, at 8. Whether CUSP's extensive contacts with the City of New York might make it a state actor for some purposes is unclear, but in general it is increasingly difficult to persuade a court that a private actor should be seen as state actor.

ions.[44] Purpose-built sensors can be placed on city-owned property and combined with legally required data collection projects and with data drawn from other devices whose owners would agree to share data in order to create a 'smart city.' These break down into three categories:

1) *New sensors designed to photograph the city from vantage points on some of the tallest buildings.* These buildings provide sight lines that cumulatively cover a large fraction of New York: about a million people are within the range of the sensors on a single tall building.[45] Sensors mounted on these buildings will be capable of covering the entire light spectrum, including infrared and spectral imagery, and will include seismic and acoustic devices, detectors for ionizing radiation, or biological or chemical agents.[46] At some point, it becomes possible to collect and collate enough data to make fine-grained deductions about individual behavior. Today, for example, the data from these sensors can be combined with other data sets to detect when rented apartments are being occupied by more than the permissible number of tenants.[47]

2) *So-called "organic data flows," which are data streams that are currently collected either in the course of business or to comply with regulatory requirements.* These data streams range from transactional information (e.g. point of sale) to operational data (traffic, transit, utilities) to administrative data on permits issued (e.g. construction).[48] Some of these databases are already surprisingly detailed. For example, New York law requires taxis to record the location of every pickup and dropoff, allowing construction of detailed pictures of the ebb and flow of taxi-riders' movements in the city.[49] Using only the starting and ending addresses of taxi journeys, one analyst deduced the identities of likely visitors to strip clubs;[50] taking the same data, plus some photos of celebrities getting in or out of taxis, allowed the analyst to show how much the celebrities tipped (nothing, apparently).[51] Similar journey information is becoming available about every car in New York now that more police cars are

44. CUSP Promise, *supra* note 40, at 15.

45. *See id.* at 4–5. How many of that million are actually detectable varies depending on what blocks the view, a problem known as 'shadowing'. Even so "a single sensor can cover [approximately] half a million people at once." Koonin Presentation, *supra* note 43, at 15:30.

46. Koonin Presentation, *supra* note 43, at 13:16. New York City is expected to be one of the major 'customers' of CUSP's databases. *Id.* at 1:08.

47. *See* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 186–89 (2013) (discussing how New York building inspections raised efficiency from 13% to 70% based on correlations between 17 existing data sets).

48. Koonin Presentation, *supra* note 43, at 6:16–:40.

49. In addition to the flow in and out of neighborhoods, the data reveal that people are more likely to get in taxis on streets, but more likely get off on avenues. *Id.* at 12:20–:30.

50. *See* Atockar, *Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset*, NEUSTAR RES. (Sept. 15, 2014), http://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/.

51. *Id.*

equipped with automatic license plate readers that can read 1,000 plates per minute.[52]

3) *Distributed sensors, a category that includes CCTV, ATM video cameras, red-light cameras, cell phones,*[53] *and fixed distributed information-gathering devices.*[54] In addition to real-world sensors, people are in effect virtual sensors when they post geotagged information about their movements and activities or that of others whom they observe, be it on Twitter, Foursquare, Facebook, or other online social software.

The details matter. There are, for example, a variety of ways one could engineer the capture of noise information from cell phones or building sensors.[55] Some might not harm privacy if they just measured decibels. Others invite misuse: anything that captured the actual sounds, whether via live streaming or recordings, would be problematic, and only more so when one considers that the information would perforce be geotagged. Add in information about the identity of the source such as the unique identifier of the phone, and one has movement records of the owner. Add in voiceprint capability, and police investigations will take on a wholly new look. CUSP has not proposed recording voices or doing voiceprinting.[56] But law enforcement, security agencies, or others seeking to market to them, would have different priorities and goals if they had access to this technology.

New York—and then other domestic and foreign cities to whom CUSP's industrial partners will inevitably sell data-gathering techniques and packages—will be able to optimize operations such as traffic flow, utilities load and service distribution. They will use the data to monitor infrastructure conditions, better plan zoning, public transit and utilities, improve regulatory compliance (i.e. "nudge"[57] or sanction law-breakers), and monitor public health including "nutrition, epidemiology, [and] environmental impacts."[58]

Because CUSP is based in a United States university that accepts government research money, the millions of third parties who could become its unwitting research subjects are also protected by an institutional mechanism. Before CUSP collects personally identifiable information it must clear its research projects with NYU's Institutional Review Board

52. Koonin Presentation, *supra* note 43, at 8:17–8:26; *see also* Andy Kessler, *In the Privacy Wars, It's iSpy vs. gSpy*, WALL ST. J. (Jan. 3, 2013, 7:16 PM), http://online.wsj.com/article/SB10001424127887323984704578206063994711952.html.

53. CUSP Promise, *supra* note 40, at 4; *cf.* Annie Karni, *A First Look at NYU's Big Data Campus*, CRAIN'S (Feb. 20, 2013, 12:01 AM), http://www.crainsnewyork.com/article/20130220/TECHNOLOGY/130219897 (quoting Dr. Koonin as explaining that he would start to tackle the urban noise problem by developing an app to use cellphones as noise meters, allowing him to put noise meters out in the city, in intersections, or on the sides of buildings).

54. Koonin Presentation, *supra* note 43, at 14:00–15:30.

55. *See* Karni, *supra* note 53.

56. *See* CUSP Promise, *supra* note 40 (noting the current noise project is focusing on measuring and characterizing noise).

57. RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2009).

58. CUSP Promise, *supra* note 40, at 6–7.

("IRB").[59] IRB reviews are the main mechanism by which universities ensure than any research involving human subjects is subjected to ethical review,[60] although the efficacy of this review is debated.[61] CUSP, thus, faces a potentially substantial obstacle to collecting large amounts of very personal data. Private mass surveillance projects not based in universities and not reliant on federal academic research grant money do not encounter this constraint.

Several United States cities have comprehensive private surveillance plans. The city of New Orleans, for example, tried to create a network of city-owned surveillance cameras but found it could not afford the manpower to review the footage and thus abandoned the plan in 2010.[62] In its stead, citizens in the Eighth District of New Orleans concerned about crime have built a privately owned network of 1,200 or more cameras deployed on private property and at private expense.[63] The surveillance images are not linked to police offices in real time, but the locations are provided to the police on a "secret Google map" and the images are available to the police upon request.[64] A similar network exists in Philadelphia.[65]

In the very near future, data collected from real-world sensors will routinely be linked to personal information available online. Real-time

---

59. GOLDSTEIN, *supra* note 42, at 22.

60. The Federal Policy for the Protection of Human Subjects (the "Common Rule") is codified in separate regulations by seventeen federal departments and agencies, including the Department of Health and Human Services ("HHS") and the Food and Drug Administration ("FDA"). The federal government and other grant-giving bodies commonly require IRB review as a condition of the grant. *See, e.g.*, *Institutional Review Boards Frequently Asked Questions*, U.S. FOOD 7 DRUG ADMIN. (June 25, 2014), http://www.fda.gov/regulatoryinformation/guidances/ucm126420.htm.

61. For examples of arguments that IRBs systematically under-regulate see Carl H. Coleman, *Rationalizing Risk Assessment in Human Subject Research*, 46 ARIZ. L. REV. 1, 3 (2004); Barbara Evans, *Ethical and Privacy Issues in Pharmacogenomic Research*, *in* PHARMACOGENOMICS: APPLICATIONS TO PATIENT CARE 328 (Howard L. McLeod et al. eds., 2d ed. 2009). *See also* Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators, 76 Fed. Reg. 44,512, 44,512 (proposed July 26, 2011) (to be codified at 45 C.F.R. pt. 46, 160, and 164) ("Although the regulations have been amended over the years, they have not kept pace with the evolving human research enterprise, the proliferation of multisite clinical trials and observational studies, the expansion of health services research, research in the social and behavioral sciences, and research involving databases, the Internet, and biological specimen repositories, and the use of advanced technologies, such as genomics."). For examples of arguments that IRBs systematically *over*-regulate see Scott Burris, *Regulatory Innovation in the Governance of Human Subjects Research: A Cautionary Tale and Some Modest Proposals*, 2 REG. & GOVERNANCE 65, 67–68 (2008); Robert Charrow, *Protection of Human Subjects: Is Expansive Regulation Counter-Productive?*, 101 NW. U. L. REV. 707, 708–09 (2007); Philip Hamburger, *Getting Permission*, 101 NW. U. L. REV. 405, 405 (2007) (suggesting that IRBs are "so sweeping a system of licensing speech and the press that it is reminiscent of the seventeenth century, when Galileo Galilei had to submit to licensing and John Milton protested against it."); Todd J. Zywicki, *Institutional Review Boards as Academic Bureaucracies: An Economic and Experiential Analysis*, 101 NW. U. L. REV. 861, 861 (2007).

62. Adrianne Jeffries, *The Camera Next Door: How Neighbors Watch Neighbors in New Orleans*, THE VERGE (Nov. 12, 2013, 11:59 AM), http://www.theverge.com/2013/11/13/4842150/new-orleans-safecams8-citizen-surveillance.

63. *See id.*; *SafeCams8*, FRENCH QUARTER MGMT. DISTRICT, http://fqmd.org/safecams8-nopdfix.html (last visited Apr. 3, 2015).

64. Jeffries, *supra* note 62, at 1.

65. *See Philadelphia Police Safecam*, PHILA. POLICE DEPT., https://safecam.phillypolice.com/ (last visited Apr. 3, 2015).

photos can rapidly be linked to online data.[66] Indeed, Google Glass's NameTag application, which has not yet been released to the public, would offer just that: invoke it when looking at a stranger, capture their photo, and within seconds the app will return whatever personal information Google thinks it knows about them, including their name, age, occupation, and whether they are listed in the national sex offender registry.[67] The National Institute of Standards and Technology ("NIST") estimates that the most accurate face recognition algorithm has a 92% chance of identifying an unknown subject in a database of 1.6 million criminal records.[68] This trend to tie real-world sensor data and virtual data to real-life identities converges with increasing real-life self-monitoring, ranging from medical data to personal cameras. Self-surveillance is even being marketed to consumers as a way to reduce insurance premiums.[69]

In short, sensors in public—whether 'public' or 'private' in law—will soon be capable of turning cities into a real first approximation of the Panopticon that privacy advocates, echoing Foucault,[70] have been warning about for many years. Linked with private sensors and self-monitoring, these data streams will converge into a giant pool of big data waiting to be mined, and to be used in ways unforeseen by the subjects of the known and unknown surveillance.[71] They raise the specter of chilling effects on speech and association.[72] As a result of these and other linkages between the real and the virtual, the privacy implications of real-world sensors take on a new importance. (The issue of purely virtual surveillance is addressed below.) That these linkages are not visible and not reasonably foreseeable are core parts of the argument that the surveilled are victims of a significant and growing failure in the market for privacy.

---

66. Alessandro Acquisti et al., identified people in minutes, using only a cell phone camera by comparing the camera picture to a database of Facebook photos. Alessandro Acquisti et al., *Faces of Facebook: Privacy in the Age of Augmented Reality* (Aug. 4, 2011) (unpublished study), *available at* http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/.

67. *See* Betsy Morais, *Through a Face Scanner Darkly*, NEW YORKER (Feb. 1, 2014), http://www.newyorker.com/tech/elements/through-a-face-scanner-darkly.

68. PATRICK J. GROTHER ET AL., NAT'L INST. STANDARDS., REPORT ON THE EVALUATION OF 2D STILL-IMAGE FACE RECOGNITION ALGORITHMS 2 (2011), *available at* http://www.nist.gov/customcf/get_pdf.cfm?pub_id=905968. However, speed and accuracy drop as the data set grows. *Id.* (noting that accuracy decreases linearly with the logarithm of the population size).

69. *E.g.*, *Snapshot*, PROGRESSIVE, http://www.progressive.com/auto/snapshot-how-it-works/ (last visited Apr. 3, 2015).

70. MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 200 (Alan Sheridan trans., Vintage Books ed. 1979) (1977).

71. Even worse, some of the uses may be secret and illicit. *See, e.g.*, Kreimer, *supra* note 4, at 150–51 (describing Senator Joe McCarthy threating citizens with exposure of private facts, and 1960's FBI COINTELPRO operation that sought embarrassing information on the administration's political opponents).

72. "Vulnerability can arise not only from the observation of dissident activities, but from sufficiently penetrating documentation of non-political transgressions." *Id.* at 151.

B. Privacy-Destruction as Market Failure

There have been many attempts to model the market for privacy. Richard Posner suggested that privacy was not an end in itself, but only a means to other things, an intermediate good.[73] Treating privacy as an intermediate good opens it up to the claim that privacy is by its nature inefficient, because privacy allows persons to conceal disreputable facts about themselves and to shift costs of information acquisition (or the cost of failing to acquire information) to those who are not the least-cost avoiders.[74] Oddly, however, Posner also concluded that data concealment by businesses is generally efficient, as allowing businesses to conceal trade secrets and other forms of intellectual property tends to spur innovation.[75] Similarly, the very concept of privacy has been challenged philosophically as nothing more than a cluster of rights better understood as property rights and bodily integrity rights.[76]

Even if one rejects these views and treats privacy as something that people desire for itself, something that has independent value, it is still hard to model and difficult to value. Privacy is not a simple commodity that most people in developed countries can go to the store and purchase.[77] It is an outcome of a set of practices and choices, many of which are not in the consumer-citizen's control.

The economic picture gets more complex, and a little less unrealistic, when one relaxes the assumption of perfect markets. Once one allows in common types of market failure it becomes easier to see why people might not just say they care about privacy, but might actually mean it, while still acting in ways that result in privacy-harming outcomes. Markets for privacy fail for several synergistic reasons, among them lack of transparency as to who is collecting data, consumer myopia as to the value of personal data, prohibitive transaction costs blocking market solutions to many information-acquisition and information-processing problems[78] and the outright absence of markets for others.

---

73. *See* Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 394 (1978).

74. *Id.*

75. *Compare* KIM LANE SCHEPPELE, LEGAL SECRETS: EQUALITY AND EFFICIENCY IN THE COMMON LAW 43-53, 111–26 (1988); *with* Edward J. Bloustein, *Privacy Is Dear at Any Price: A Response to Professor Posner's Economic Theory*, 12 GA. L. REV. 429 (1978); *and* James Boyle, *A Theory of Law and Information: Copyright, Spleens, Blackmail, and Insider Trading*, 80 CAL. L. REV. 1413, 1443–57, 1471–77 (1992).

76. *See* Judith Jarvis Thomson, *The Right to Privacy*, *reprinted in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 272, 280–81 (Ferdinand David Schoeman ed., 1984). *But see* JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 28–39 (1992) *and* Thomas Scanlon, *Thomson on Privacy*, 4 PHIL. & PUB. AFF. 315, 315 (1975). While I prefer to view privacy as a free-standing human right rather than as a form of property right, I would argue that the thesis of this paper is entirely consistent with a property rights-based privacy paradigm.

77. It is undoubtedly true that a substantial amount of privacy is available if one is rich enough—think Howard Hughes—or willing to be reclusive enough ("live off the grid"); *cf.* J.J. LUNA, HOW TO BE INVISIBLE (3d ed. 2012).

78. For an early discussion of these issues see Peter Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *in* PRIVACY AND SELF-REGULATION

Familiar models, drawn from property law, from environmental law, and from the economics and psychology of information, illustrate these and other problems.

1. Sensing as Externalities

Technologies that record information about persons in public and that track online behavior across multiple web sites or across multiple social media outlets are best understood as externalities.[79] Most data captured in (or through[80]) public places are not based on any contractual relations. In contrast, online surveillance may sometimes have been mentioned somewhere in a contract between the data subject and someone, but that contract likely never had meaningful assent from that person, especially if it was a "clickwrap" or "webwrap" contract in which no money changed hands.[81] In fact, the contract likely never got read at all.

As technologies for collecting, storing, and collating information about what others do improve and proliferate, the cost of amassing and analyzing this data has fallen dramatically.[82] Much of this information (e.g. one's movements in the city or the amount of heat emanating from an apartment) may have been formally accessible to a few individuals, but most of them did not care and almost none of them would store, share, or analyze the data. The acts of collecting, collation, and analysis all reduce the privacy of the subjects of the monitoring. This loss of privacy is, in effect, an external cost—or, in other cases, an external benefit[83]—to those persons.

The classic economic answers to an externality are either to attempt to internalize it or to attempt to invoke the Coase Theorem.[84] Both ap-

---

IN THE INFORMATION AGE BY THE U.S. DEPARTMENT OF COMMERCE 3–4, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=11472.

79. *See* Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 10 (2006); *see also* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 7–8 (1998).

80. This parenthetical caveat includes cameras and other sensors that routinely penetrate into the home, whether through the windows or through the walls, after traversing public spaces. It does not include the actions of a 'peeping tom' nor does it include a sensor located inside the curtilage of the home, and aimed at the inside of the home—so long as that sensor is controlled by the resident or was explicitly approved by the resident.

81. *See generally* MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2013).

82. *See Froomkin*, *supra* note 8, at 1472.

83. An example of an external benefit of lost privacy due to monitoring would be the public health value of tracking, and perhaps blocking, the spread of an epidemic. For other hoped-for benefits of the "Smart City," see generally ANTHONY M. TOWNSEND, SMART CITIES: BIG DATA, CIVIC HACKERS, AND THE QUEST FOR A NEW UTOPIA (2013).

84. The lawyers' version of the Coase Theorem, that as a general matter parties will reach an economically efficient result regardless of the assignment of property (or other) rights and that henceforth regulation of externalities tends to cause economic losses, is based on an over-generalization of the argument in Ronald Coase, *The Problem of Social Cost*, 3 J. L & ECON. 1 (1960). For a useful corrective entirely within the law and economics tradition see Steven G. Medema & Richard O. Zerbe, Jr., *The Coase Theorem, in* ENCYCLOPEDIA OF LAW AND ECONOMICS 836, 875–76 (1999) (concluding

proaches flounder here due to the size of the transaction costs involved in making agreements with potentially millions of surveilled subjects and/or the difficulties of valuation and the amount the data subject would need to spend to acquire enough information in order to make a good decision about the long-term consequences of sharing data.[85] As further described below in Section II.C, private law does not offer remedies to those who suffer a negative externality from having their personal information collected and used. Even if it did, however, collective action problems and the relatively high costs of litigation compared to the value of any one person's data make the transactions costs so great that the Coase Theorem would be inapplicable.[86] One cannot bargain in the shadow of the law if the law's shadow is invisible.

2. *Tragedy of the Information Commons?*

It could be argued that our property rights regime assigns the right to gather information in a privacy 'commons' akin to Garret Hardin's famous grassy space overgrazed by sheep.[87] It makes for a powerful metaphor, but is not quite as technically accurate as the straightforward externality account.[88]

A true commons may be held in commons by a community; in contrast, no one formally 'owns' the rights to the privacy-value of personal information observable in or through public spaces. That information is, as a practical matter, initially controlled by the data subject, but once it is

---

that the Coase Theorem is formally correct, unrealistic, and does not in fact support the majority of policy proposals frequently associated with it).

85. One might also wonder at the cognitive load that making a daily series of those decisions likely would impose on anyone who tried to do it.

86. As discussed below, in Part IV.A, the First Amendment imposes strict constraints on any attempt to craft more powerful private remedies via statute. Only if, counterfactually, we could craft private law remedies for the privacy lost from information collection in or through public places, could we then profitably discuss removing additional impediments to a litigation remedy, including defining the entitlement, whether one should assign the entitlement to the least-cost avoider (presumably the collector in most cases), how to aggregate claims for litigation or bargaining, and how to overcome information asymmetries between collector and surveilled.

87. Garrett Hardin, *The Tragedy of the Commons*, 162 SCI. 1243, 1244 (1968). Hardin's account is not without its critics, *e.g.*, Elinor Ostrom et al., *Revisiting the Commons: Local Lessons, Global Challenges*, 284 SCI. 278, 278 (1999); *see also* Michael A. Heller, *The Tragedy of the Anticommons: Property in the Transition from Marx to Markets*, 111 HARV. L. REV. 621, 624 (1998). It also may not be historically accurate, PARTHA DASGUPTA, HUMAN WELL-BEING AND THE NATURAL ENVIRONMENT 129 (2001), but it remains a handy metaphor. For a useful analysis of the 'tragedy' in the tragedy of the commons see Shi-Ling Hsu, *What Is a Tragedy of the Commons? Overfishing and the Campaign Spending Problem*, 69 ALB. L. REV. 75, 78–79 (2005).

88. Here I part company with Hirsch, who endorses the commons metaphor, Hirsch, *supra* note 79, at 10, largely because he defines the commons as the trust people have in each other to respect privacy; losing that trust undermines the "collective willingness of individuals to reveal their personal information." *Id.* at 29. I do not think that definition is useful, perhaps because I think that trusting others not to misuse self-posted information is very optimistic. Expecting people not to capture and digitize one's activities in public may also be a misplaced expectation, but that only strengthens the case for regulation. One of Hirsch's examples, spam email, *id.* at 15, 43–48, does seem like a commons problem but does not seem like a privacy issue in the sense I am using the term—control over data about oneself. It is a privacy issue in the sense of other definitions that, like the classic privacy tort, include intrusion upon seclusion, or intrusion upon mailbox.

visible to others it is owned in a non-rivalrous way and is capable of being copied and used at any time by any observer. To the extent that the diminishment of privacy in public spaces or online is caused by users taking pictures of each other and then posting them online, we do have a closer analogy to the classic tragedy of the commons: everyone is drawing from the common stock of public privacy.[89] And perhaps everyone, or at least many people, may have an incentive to reduce the common stock of privacy in order to gather more 'likes' or 'followers.'

On the other hand, to the extent that the privacy diminishment is imposed by a third-party data-gatherer, one perhaps unknown to the data subjects, I think the language of externalities best captures the relationship. Again, there is no bargained-for exchange; indeed, there may be no relationship other than that the person being photographed and analyzed happens to pass by a camera on the side of the building or happens to walk in the line of sight of a sensitive detector placed on the roof of a far-away skyscraper. The absence of any relationship distinguishes these situations from related, but distinct, scenarios such as a cell phone contract in which the surveillance is incident to an actual legal contract (even if one governed by boilerplate and thus not classically bargained-for) in which the subject gets clear notice of, say, the cell-phone company's intention to collect location data. That too is a serious privacy issue, and may be problematic on several levels, but it is not formally the imposition of an externality.

It may seem odd to some to talk of externalities without first defining a property right, but in fact this is not at all odd in the environmental realm. We use externalities to analyze air pollution in public places without necessarily specifying who owns the right to breathe what air. Similarly, we talk of greenhouse gas emission as an externality without specifying who exactly owns the right to avoid global warming. Alternately, if it is essential to specify property rights, we could just say that data concerning acts in public are not owned at all. Or, they could be said to belong jointly and severally to everyone capable of observing them. Similarly, one might question whether it is right to talk of an 'externality' when speaking of a relationship that could be described as dyadic.[90] In the classic externality case, the first party does something (e.g. plant flowers, emit pollution) without regard to the consequences for others who then enjoy (more honey) or suffer (more cancer) the consequences. In the case of surveillance, the first party does something (e.g. set up a data collection device) precisely in order to do something to someone else (capture their data). The privacy harm, as well as any resulting pub-

89. *Cf.* Lior Jacob Strahilevitz, *Collective Privacy, in* THE OFFENSIVE INTERNET: PRIVACY, SPEECH, AND REPUTATION 217 (Saul Levmore & Martha C. Nussbaum eds., 2010). In collective privacy situations, problems arise "where a single source of confidential information reveals something about multiple individuals, and these people disagree over whether the information should be disseminated." For example, one individual tags multiple people in a photograph posted on Facebook and then sets privacy controls so loosely that the information is publicly revealed. *Id.*

90. I'm indebted to Leigh Osofsky for raising this question.

lic benefit, is not, it could be argued, an 'externality' but rather the essence of the transaction. (In a pollution case, we do not see the polluter collecting the effluent for profit.) I think this characterization, which flows from the non-rival nature of data,[91] misses the point. If the parties being surveilled care about their privacy, then the surveilling party is imposing an un-bargained for cost on his target in order to achieve an end of his own. Whether or not that perfectly fits the classic model of an externality, it can certainly be modeled as one.[92]

3. *Information Asymmetries*

Not only are consumers in a poor legal position to complain about the third-party sale of data concerning themselves,[93] but often they are not in any position to even understand the likely consequences of sharing data about themselves.[94] Part of this is that the long-term consequences are in many cases not knowable: few if any would have predicted in 1997 that putting personal information on a web page would lead to it being harvested for consumer and law enforcement profiles. Even when the long-term consequences are knowable, it may be unreasonably expensive to game out all the possible scenarios. Indeed, it is difficult if not impossible for an ordinary person to stay informed as to the contemporary uses of even innocuous-seeming personal data.[95]

This "myopia" about the long-term consequences—a systematic inability to correctly value personal data—explains much of why people tend to say they care about their privacy but nonetheless often act as if they do not. (Other explanations are lock-in[96] and bounded rationality.[97])

---

91. *See* James B. DeLong & A. Michael Froomkin, *Speculative Microeconomics for Tomorrow's Economy*, in INTERNET PUBLISHING AND BEYOND: THE ECONOMICS OF DIGITAL INFORMATION AND INTELLECTUAL PROPERTY 6 (Brian Kahin & Hal Varian eds., 2000).

92. What is more, the costs imposed can be beyond the value of the datum because if one does not know the nature, number, and location of the sensors then the cost of counter-measures for the very privacy conscious could be very high. Thus, the cost is not simply extractive; in the face of an unknown, perhaps immeasurable, threat, it might include the expenditures for considerable self-help protection.

93. For an extreme example, see Moore v. Regents of the Univ. of Cal., 793 P.2d 479, 488–97 (Cal. 1990) (holding that a patient had no cause of action, under property law, against his physician or others who used the patient's cells for medical research without his permission).

94. An earlier version of some of the ideas in this sub-section appears in Froomkin, *supra* note 8, at 1501–04.

95. For confirmation of this assertion one need only look at the horrified reactions of consumers to the discovery that changes in their buying patterns could alert Target to life changes such as pregnancy, see Charles Duhigg, *How Companies Learn your Secrets*, N.Y. TIMES MAG. Feb. 16, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html. It is not widely known that credit card companies can predict divorce by buying patterns. *See* IAN AYRES, SUPER CRUNCHERS: WHY THINKING-BY-NUMBERS IS THE NEW WAY TO BE SMART 36, 197 (2007).

96. Information sharing requests sometimes come in situations that involve very high switching costs. For example, even if a consumer was aware of the consequences when Google changed its terms of service to allow information sharing among its products, the cost of leaving the Google ecostructure might have meant changing one's email address, not to mention other common Internet tasks. E-mail from Jonathan Baker, Professor of Law, American Univ., to Michael Froomkin, Professor of Law, Univ. of Miami, Feb. 7, 2014 (on file with author).

It also seems a likely explanation for the current raft of (over)sharing in social media, which some have termed "self-surveillance."[98] The valuation problem is vastly worse when there is nothing to signal that the surveillance is occurring: if consumers are not able to correctly value their privacy when, say, signing standard form contracts, how can we expect them to make reasonable, much less optimal, privacy choices when it is next to impossible for them to even know that a camera is watching them from a tall building far away?

In the ordinary transaction, be it a sale or a social encounter, the fact of the transaction ordinarily belongs equally to each participant,[99] and both sides to a transaction ordinarily are free to sell details about the transaction to any interested third party. There are exceptions to this rule (e.g., fiduciary duties and a lawyer's duty to keep a client's confidence),[100] but compared to the overall number of transactions, they are relatively rare.

Parties to a transaction could in theory contract for confidentiality. Consumers do not do this for two sets of reasons. First, the cost of negotiating in a world of standard forms is very high.[101] Similarly, there is also a high cost associated with attempting to impose contracts on relationships that are non-economic and ordinarily non-contractual (e.g., being observed by one's neighbors).[102] Second, even if the transactions costs were low or non-existent, consumers would tend to sell their data too often and too cheaply.[103]

A simple model explains why it is that Americans really will sell their privacy for a frequent flyer mile, at least for ordinary consumer transactions as opposed to extraordinary private ones, such as sensitive health-related matters. Assume that a representative consumer engages in a large number of transactions. Assume further that the basic consumer-related details of these transactions—consumer identity, item pur-

97. Arguably, even if people suddenly had perfect information about the devices that watch them they would not be able to use that information well. The simplest form of the bounded rationality claim has to do with the amount of time it would take to process all the information and make rational decisions. *See* OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE, 107–18 (2014). More far-reaching forms of the claim invoke various cognitive limits constraining our ability to weigh risks and uncertainties, *see* DANIEL KAHNEMAN, THINKING, FAST AND SLOW (2011); Herbert Simon, *Theories of Bounded Rationality*, in DECISIONS AND ORGANIZATION 161 (C.B. McGuire and Roy Rader eds. 1972); Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. REV. 1203 (2003); Owen D. Jones, *Time-Shifted Rationality and the Law Of Law's Leverage: Behavioral Economics Meets Behavioral Biology*, 95 NW. U. L. REV. 1141 (2001), and our tendency to overoptimism. KAHNEMAN, *supra*.

98. *See supra* Part II.A.2.

99. *See* Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 446 (1995) (noting the traditional view, now retreating in Europe, that "data . . . were perfectly normal goods and thus had to be treated in exactly the same way as all other products and services").

100. *See* MODEL CODE OF PROF'L RESPONSIBILITY CANON 4 (1980); MODEL RULES OF PROF'L CONDUCT RULE 1.6 (2013).

101. *See* Radin, *supra* note 81, at 15–16.

102. *Id.* at 31–32.

103. *See* Froomkin, *supra* note 8, at 1502.

chased, cost of item, place and time of sale—are of roughly equivalent value across transactions for any consumer and between consumers, and that the marginal value of the data produced by each transaction is low on its own. Assume also that the merchant's marginal cost of collection of consumer data in a form suitable for sale is effectively zero since they are routinely collected for other internal purposes. So far, none of these mostly very standard assumptions should be controversial.

Now add the key assumption: aggregation adds value. In other words, once a consumer profile reaches a given size, the aggregate value of that consumer profile is greater than the sum of the value of the individual data standing alone. Most heroically, assume that once some threshold has been reached the value of additional data to a potential profiler remains at least linear; it does not decline.

In a world where information exchange about consumers has these properties, it follows that data brokers or profile compilers will be able to buy consumer data from merchants at low transactions costs, because the parties are repeat players who engage in numerous transactions involving substantial amounts of data. It also follows, however, that consumers will be unaware of the value of their aggregated data to a profile compiler because those transactions and valuations are invisible to them.

We would usually expect a consumer to value a datum at its marginal value in lost privacy. Given the limits on the consumer's knowledge that datum will seem to be worth only its lower, un-aggregated, value. But the merchant—who foresees selling that datum to a profiler—will value the datum at its higher, aggregated value as part of a profile, because in an efficient market that is what the profiler will be willing to pay for it. Given the assumptions above, that amount, the aggregated value of the datum to the profiler, will always be greater than the un-aggregated value of that same datum to the consumer because aggregation adds value. It follows that a rational consumer, faced with what appears to be an attractive offer, will always be willing to sell data at a price that a merchant is willing to pay.

Alternately, one could posit that the market for information brokerage services likely has oligopolistic tendencies that would tend to push the price of a datum below the aggregated value, although perhaps not as low as the un-aggregated value. The increased value caused by aggregation is an economy of scale that benefits the data broker. If the economies of scale are substantial, in the long run we can expect an oligopolistic market structure in which a few large data aggregators collect and resell information, and the need to aggregate would create a barrier to entry that protects incumbents from new competition. If there were only two parties to the information transaction, the negotiated price of recorded information would likely end up somewhere in a range between the non-aggregated and the aggregated value.[104]

104. Baker e-mail, *supra* note 96.

Even if this consumer myopia is real, or if the market structure for information brokerage is as oligopolistic as suggested, how much we care depends primarily on the intrusiveness of the profile.[105] Privacy myopia is an increasing problem, as more aggregation creates widespread aggravation.[106] On the other hand, if people who object to being profiled are unusual, the main consequence of privacy myopia is likely distributional. Consumers who place a low value on their information privacy would have agreed to sell their privacy even if they were aware of the long-run consequences. The only harm they suffer is that they got a lower price than they would have demanded had they understood the value of what they were giving up. Meanwhile, however, consumers who value information privacy most highly will be most seriously harmed by their privacy myopia. Had they but known the aggregated value of each datum, they would not have sold at all.

Transaction costs only make this worse. When the consumer's marginal value[107] of a given datum is small, then the value of not disclosing that datum will in most cases be overshadowed by the cost of negotiating a confidentiality clause (if that option even exists) or the likely higher cost of forgoing the entire transaction.[108] Thus, in ordinary cases where the datum does not seem extraordinarily revealing on its own, privacy clauses are unlikely to appear in standard form contracts, and consumers will accept this.[109] Nor would changing the law to make consumers the default owners of information about their economic activity tend to produce confidentiality clauses. In most cases, all it will do is move some of the consumer surplus from information buyers to information producers or sellers as the standard contract forms add a term in which the consumer conveys rights to the information in exchange for a frequent flyer mile or two.

Thus, if (1) consumers are plausibly myopic about the value of a datum because they are focusing on the datum's marginal value rather than its difficult-to-measure average value, and (2) profilers are not myopic in this way because they can estimate the average value of the datum as part of their aggregate data and the data are more valuable in the aggregate, then there will be substantial over-disclosure of personal data even when consumers care about their informational privacy.

---

105. Theoretically, it might depend secondarily on the value of the difference in price between the transaction price and its market value under perfect competition, but in the absence of further data we do not now have reason to believe that even the aggregated value at the aggregated price creates a serious issue of wealth transfer from the consumer to intermediaries or the aggregator.

106. *See* Froomkin, *supra* note 8, at 1502.

107. Or even the average value to a well-informed consumer.

108. *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 519–23 (1995); Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1067 (1999) (arguing that consumers' transaction costs in protecting their privacy may be inflated by businesses).

109. *See* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2413 (1996) (noting that "[e]ven the most resolute consumer will confront form contracts that are (generally) not subject to dickering over individual terms.").

If this depiction of privacy myopia is even somewhat accurate, it suggests that proposals to change the default property rule regarding ownership of personal data in ordinary transactions will not achieve much.[110] The data sale will tend to happen even if the consumer has a sole entitlement to it. It also suggests that European-style data protection rules will be effective for highly sensitive personal data, but less so for lower-value data. The European Union's data protection directive allows personal data to be collected for reuse and resale if the data subject agrees;[111] the privacy myopia story suggests that customers will ordinarily agree to the sale except when disclosing particularly sensitive personal facts with a visibly higher marginal value.

An equally significant problem arises when the subject is aware of the surveillance but either powerless to prevent it, or only able to do so at exorbitant cost. For example, consumers could be notified that their energy usage is being monitored, and that the monitoring is so sensitive that it can identify the model of their appliances and even the TV show they are watching.[112] There is not that much, however, the average consumer could do with this information. Consumers could switch, whenever possible, to battery operated devices that run on batteries charged by a generic battery recharger. But that will not work for large appliances.[113]

Similarly, apartment renters in New York who do not want their heat emanations to be detected[114] are in practical terms unable to insulate apartments they do not own; even if they owned them, they likely would not be able to make the structural adjustments to the apartment at a reasonable cost (and without upsetting the Co-op Board or other management). If the information were only aggregated, they might not suffer any consequences; but sensors can or will be able to identify each apartment,

110. Classically, who a tax burden is placed on does not change the division of the surplus; only the relative elasticities of supply and demand do that.

111. *See* Viktor Mayer-Schönberger, *Generational Development of Data Protection in Europe, in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 219, 231–232 (Philip E. Agre & Marc Rotenberg eds., 1997).

112. *See* California Smart Grid, *supra* note 25. For a U.K. perspective on similar issues, see J. Savirimuthu, *Smart Meters and the Information Panopticon: Beyond the Rhetoric of Compliance*, 27 INT'L REV. OF L. COMPUTERS & TECH. 161, 161 (2013).

113. I have been told of one engineer who experimented with installing a "noisemaking" device between his house and the electrical supply. Using a series of large batteries he both drew random charges from the batteries to reduce his draw on the electrical grid, and also randomly drew extra current to replenish the batteries. The experiment, I was told, successfully masked the electrical signatures of the home, but nonetheless failed because the constant charging and discharging of small amounts of electricity rapidly destroyed the batteries. Not only does this sort of masking require skills unavailable to the average consumer, but it appears to be ridiculously costly in that it quickly damages the (expensive) batteries. *Cf.* MAREK JAWUREK,ET AL., PRIVACY TECHNOLOGIES FOR SMART GRIDS–A SURVEY OF OPTIONS 13 (Microsoft 2012), http://research.microsoft.com/pubs/178055/paper.pdf and Michael Backes & Sebastian Meiser, *Differentially Private Smart Metering with Battery Recharging, in* DATA PRIVACY MANAGEMENT AND AUTONOMOUS SPONTANEOUS SECURITY, 194, 201 (Joaquín García Alfaro ed, 2012) *available at* http://eprint.iacr.org/2012/183.pdf.

114. *See supra* notes 46–47 and accompanying text (discussing what can be learned from measurements of infrared and light emissions from a large majority of New York City offices and apartments).

and will be able to correlate that information with other data to reach conclusions about its inhabitants.

The privacy myopia problem is even more obvious when the subject of data collection is not aware that she is being surveilled. Indeed at that point, the term 'myopia' seems inappropriate, as the problem is no longer impaired vision, but either blindness or ignorance. The example of heat emanations from apartments is ironic here because the measurement of heat emanations is exactly what Danny Kyllo complained of, and the Supreme Court said that was a search that required a warrant.[115] But when the measurement is by a private party, at a distance, and at a mass scale, it is unlikely to be held to be either a criminal trespass or a privacy tort, and in any event few, if any, apartment-dwellers will be aware of it when it happens. Then the police simply buy the data.

Like with privacy myopia, much of the privacy blindness problem is informational: lack of knowledge about the fact of the information collection or lack of knowledge about its consequences.[116] And both of these informational gaps are problems that a notice regime seems well-calculated to ameliorate and perhaps even cure.[117] Part III below thus sets out proposals based on environmental law that would require those embarking on mass surveillance projects to first give public notices designed to fill these information deficits. Before outlining those solutions, however, it is useful to explore why some current attempts to deal with mass surveillance have not been, and are not likely to be, successful.

C. Privacy Doctrine Offers Too Few Tools to Combat Mass Surveillance

Existing U.S. regulatory structures are totally unprepared for the data collection deluge. U.S. law currently has relatively few privacy-protecting rules,[118] and what exists tends to focus on data sharing rather than data collection.[119] Although courts have found a limited right to privacy in the Constitution, that right finds most of its expression in the context of bodily integrity, and the traction in the information privacy arena is speculative and limited at best.[120] Some members of the Supreme Court

115. *See infra* text at notes 128–39.

116. *See* Froomkin, *supra* note 8, at 1501–02.

117. An additional problem may be social and legal—whether the measurement is in any way tortious or should otherwise be regulated; more information about what data are being collected would inform, or even spark, a debate.

118. *See, e.g.*, James B. Rule, *The Whole World Is Watching*, 22 DEMOCRACY (Fall, 2011), http://www.democracyjournal.org/22/the-whole-world-is-watching.php?page=all (noting that the U.S. stands out among liberal democracies without an independent data-protection commission and with its comparatively restricted privacy codes).

119. *See* Robert Gellman, *Does Privacy Law Work?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 192, 215 (Philip E. Agre & Marc Rotenberg eds., 1997).

120. *E.g.* Whalen v. Roe, 429 U.S. 589, 605 (1977) (noting that the Court is "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." However, the Court concluded it does not need to "decide any question which might be presented by the unwarranted disclosure of accumulated private

have signaled an interest in an evolution of privacy law,[121] but those judicial developments are still far in the future if they are to ever come at all. Tort law has little to offer, because the classic privacy torts are somewhat limited and generally do not apply to the major data collection efforts that occur in (or through) public spaces.[122] Nor do privacy torts have much traction against the often-unseen consequences of contractual agreements, most notably those relating to cell phones and internet-based technologies.[123] Neither contract nor property-rights based approaches have to date yielded much due to a combination of factors ranging from transaction costs, to the bounded rationality of consumers, to problems inherent in domains where who-owns-what is at best contested. The fact is, it is increasingly difficult to defend one's privacy in industrialized countries; sensor technologies and data aggregation technology are winning an arms race against privacy enhancing technologies, an arms race that most consumers are only dimly aware they are involved in.

Recent opinions in *United States v. Jones*[124] and *Florida v. Jardines*[125] suggest that some members of the Supreme Court would welcome a property-based rationale that could protect enclaves of privacy, particularly the home. So far, neither case articulates a theory adequate to the mass public surveillance problem with which this article is mainly concerned: those opinions say little about privacy in public, and even less about data privacy.[126] To the extent that the cases link trespass and search, they do suggest parallel protections from public and private intrusions.[127] Increased legal protection from "intrusion" in the sense of physically coming on the property, invading the person, or entering into other private spaces, would be important and valuable, but at best will address only a fraction of the issues raised by the rise of a system of mass surveillance that involves private and public spaces. Surveillance penetrates into private spaces even when it does not peer into them. It deduc-

---

data whether intentional or unintentional or by a system that did not contain comparable security provisions.").

121. Notable recent suggestions appear in Justice Kagan's opinion in Florida v. Jardines, 133 S. Ct. 1409, 1418 (2013) (Kagan, J., concurring) (noting that while "[t]he Court today treats this case under a property rubric," she "could just as happily have decided it by looking at Jardines' privacy interests"), joined by Justices Ginsburg and Sotomayor, and in Justice Sotomayor's opinion in United States v. Jones, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring) (noting that "[t]he Government usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection").

122. *See* Froomkin, *supra* note 8, at 1535.

123. *See, e.g.*, Hennig v. Alltel Communications, Inc., 903 So. 2d 1137 (La. Ct. App. 2005) (upholding dismissal of claim for invasion of privacy against phone company that alleged phone company released patron's cellular phone records to patron's husband without her authorization, causing breakup of her marriage); *see also* Patricia Sanchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH., 1, 5 (2007).

124. 132 S. Ct. at 949 (holding that attaching GPS to car in order to monitor its movements was trespass and thus a search).

125. 133 S. Ct. at 1414 (holding that officer's bringing of drug-sniffing dog within curtilage of home was trespassory search requiring a warrant).

126. *Jones*, 132 S. Ct. at 948–54; *Jardines*, 133 S. Ct. at 1413–18.

127. *See Jones*, 132 S. Ct. at 950; *Jardines*, 133 S. Ct. at 1415.

es information about private spaces based on emanations from them. It collects data on behavior in real and virtual public places and uses those data to make inferences that not only concern private spaces, but also private thoughts and actions.

In mass surveillance, rather than being focused on particular suspects, the surveillance is widespread or even ubiquitous; the information gathered need not be, and almost never is, based on some suspicion, much less reasonable suspicion, of a criminal act by a particular person. Sometimes mass surveillance in the private sector is pursuant to some contract, although it also takes place in public without warning, as well as online in open virtual spaces. And, critically, mass surveillance almost always, perhaps inevitably, requires machines to act as sensors and to sift and sort the data those sensors collect.

Kyllo v. United States[128] involved the legality of warrantless machine-assisted (also known as sense-enhanced) surveillance.[129] Thus, even though it only addressed the limited case of targeted surveillance into the home, *Kyllo* could seem to provide a starting point for thinking about a regulatory solution to mass surveillance. In 1992, federal agents located on a public road pointed a thermal imager at Danny Kyllo's home.[130] Based on the heat emissions from his house, utility bills, and "tips from informants" the agents concluded that Kyllo was running an indoor marijuana growth operation and persuaded a magistrate to issue a search warrant leading to his arrest.[131] The issue presented to the Supreme Court was whether the use of the machine-enhanced detection of heat emanations constituted an unreasonable warrantless search or whether, as the Ninth Circuit had ruled, Kyllo's failure to attempt to conceal the abnormal heat emanations showed a lack of a subjective expectation of privacy[132] and that any such subjective expectation, in any case, would have been objectively unreasonable because the thermal imager "'did not expose any intimate details of Kyllo's life,' only 'amorphous "hot spots" on the roof and exterior wall.'"[133] Justice Scalia's majority opinion in *Kyllo* supplies an answer to the question of "how much technological enhancement of ordinary perception from [a public] vantage point, if any, is too much" for the surveillance of a home,[134] and "what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[135] The answer is that it depends on whether the device is "in general

128. 533 U.S. 27 (2001).
129. *Id.*
130. *Id.* at 29–30.
131. *Id.*
132. An infrequently mentioned difficulty for the government in *Kyllo* was that in other cases agents or police had argued that the *absence* of normal heat emanations was evidence of a covert grow facility. *See* United States v. Kerr, 876 F.2d 1440, 1443–44 (9th Cir. 1989) (considering the absence of heat a sign of suspiciously good insulation).
133. *Kyllo*, 533 U.S. at 31 (quoting United States v. Kyllo, 190 F.3d 1041, 1047 (9th Cir. 1999)).
134. *Id.* at 33.
135. *Id.* at 34.

public use."[136] If the answer is yes, then the device can be used "to explore details of the home that would previously have been unknowable without physical intrusion" without a warrant; if, however, the answer is no, then the state must get a warrant to use the device.[137]

A Supreme Court pronouncement that there are limits to how much new technology can be used to "shrink the realm of guaranteed privacy"[138] may seem like a good basis for thinking about legal limits to mass surveillance, but in fact *Kyllo*'s answer is a bad one on its own terms and, if anything, worse as applied to mass surveillance. To begin with, *Kyllo* applies directly only to surveillance of the home by the government—although trespass doctrines presumably would cover similar private sector surveillance.[139] Even within its limited domain, *Kyllo*'s expectation-based rationale cannot be a long-term solution to any privacy problem because it creates a one-way ratchet: as a technology becomes sufficiently common, we no longer have an expectation of privacy based on its non-use.[140] Therefore, under *Kyllo*'s logic, over time police can adopt any increasingly widely deployed technology without a warrant, as it will no longer be a search.[141] Presumably, similarly situated private observers will be able to do the same without fear of tort liability.

If *Kyllo* is not the answer, then it is back to the drawing board. Market failure, bounded rationality, collective action problems, and serious social consequences are the ingredients of a scenario that should invoke regulation, or at the very least a careful conversation as to whether the public interest would be served by government reform and intervention. Indeed, in many other areas of life, notably environmental regulation, the state does intervene to at least partly correct market failures (and government planning failures) that otherwise make it too cheap and too easy to pollute. Class action lawsuits are, in theory, available to redress some environmental harms, and they could seem to be a potential solution to surveillance. The reality, however, is otherwise. Even if one were to change the law to make surveillance in public tortious—a rule with potential First Amendment difficulties[142]—other obstacles would

136. *Id.*

137. *Id.* at 34–35, 40.

138. *Id.* at 34.

139. *Id.* at 40.

140. Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U.L. REV. 1381, 1382 (2008) (blaming origins of one-way ratchet on Justice Harlan's opinion in *Katz*); Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321, 2335–36 (2007) (noting the evolution of technology, specifically in the map industry, that has led to a significant erosion of privacy expectation amongst the users of the ever-evolving technology). Ratchets can work the other way too, for example, when standards of care ratchet up in response to the fear of tort liability. *See* James Gibson, *Doctrinal Feedback and (Un)Reasonable Care*, 94 VA. L. REV. 1641, 1645 (2008). *See also* Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1306 (2002).

141. *Kyllo*, 553 U.S 27 at 40. For a suggestion that the ratchet works the other way in European human rights law—"expand[ing] the meaning of private life over time but [never] contracting it"—see H. Tomás Gómez-Arostegui, *Defining Private Life Under The European Convention On Human Rights By Referring To Reasonable Expectations*, 35 CAL. W. INT'L L.J. 153, 192 (Spring 2005).

142. *See infra* Part IV.A.

remain. To begin with, any attempted class action lawsuit about privacy harms would face the same practical and procedural barriers that prevent class action suits for physical damage from toxins, including the very real problem that the plaintiffs likely experienced different exposures and suffered different harms, making class status problematic. To make matters worse, the privacy harms would in most cases be far more difficult to monetize than the lost health and life from exposure to a toxin.

If private law is not the answer, that suggests a need for regulation. That the lack of data on privacy valuation makes it difficult to do traditional cost-benefit analysis may create an argument for caution, but if we know the sign of the effect and believe it to be substantial then that may be enough to justify action. As an interim measure, the ideal regulatory scheme would provide more data on the relevant costs or benefits while heading off the greatest dangers.[143]

The major regulatory response to potentially privacy-harming technologies' developments to date is the European Union's data protection rules.[144] The centerpiece of those rules, the Data Protection Directive,[145] is currently being reviewed by the European Commission, but the proposed changes are controversial.[146] Meanwhile, neither the existing version of the Directive, nor the regulatory structures that it anchors, has achieved significant traction in the United States.[147]

EU-style regulation imposes limits on data collection and also on data re-use and data sharing.[148] One of the many obstacles to adopting a similar regime in the United States is that once information has been collected, regulation becomes more difficult: the First Amendment makes it difficult to stop people from saying true things that they know[149] unless

143. *See infra* notes 227–32 and accompanying text.

144. Council Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002 O.J. (L 201) 37–47 [hereinafter E-Privacy Directive].

145. Council Directive 95/46/EC, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, 32 [hereinafter Data Protection Directive].

146. *See, e.g.*, LIBE Committee Vote Backs New EU Data Protection Rules, Europa.eu (Oct. 22, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-923_en.htm.

147. *U.S.-E.U. Safe Harbor Overview*, EXPORT.GOV (Dec. 18, 2013, 3:45 PM), *available at* http://export.gov/safeharbor/eu/eg_main_018476.asp (noting that "the United States takes a different approach to privacy from that taken by the EU. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation" and therefore enforcement of the Safe Harbor Rule "will be carried out primarily by the private sector").

148. Data Protection Directive, *supra* note 145, at 34.

149. *See* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2656 (2011) (striking down Vermont law preventing pharmacies from selling, disclosing, or using of prescriber-identifying information as a content-based restriction on speech); Bartnicki v. Vopper, 532 U.S. 514, 528 (2001); Smith v. Daily Mail Pub. Co., 443 U.S. 97, 102 (1979); *see also* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1051 (2000) (noting the friction between First Amendment rights and Privacy rights). For a particularly stark example of what would happen if it were possible to stop people saying true things they know, see Josh Gerstein, *NSA Chief: Stop Reporters 'Selling' Spy Documents*, POLITICO (Oct. 24, 2013, 5:56 PM), http://www.politico.com/blogs/under-the-radar/2013/10/nsa-chief-stop-reporters-selling-spy-

there is a special relationship,[150] a contract, or a small number of other special cases.[151] The First Amendment block on rules that prohibit information-sharing is particularly strong if the knowledge was acquired outside of a commercial transaction. Commercial speech is somewhat easier to regulate than other kinds of speech; that rule is counter-balanced, however, by the reality that a contract imposing standard-form consent frequently governs.[152] For these and many other reasons, the adoption of EU-like rules in the United States appears unlikely in the near future.[153]

D. Understanding Surveillance as Pollution of the Private Sphere

Many mass data-collection activities, particularly those that take place "in or through public spaces" can usefully be analogized to pollution of the private sphere.[154] "In or through public spaces" includes these scenarios:

(1) Encroachments on 'privacy in public.' This category includes most technologies whether or not controlled by a participant that watch other people in public and record their actions. It includes the monitoring of personal actions while walking or driving any place outside a home, such as monitoring cell phone locations,[155] mass facial recognition technology,[156] and license plate recorders.[157] "Public" here includes not only legally public spaces such as roads and sidewalks, but also the insides of buildings commonly open to the public, such as retail stores and many government offices;

---

documents-175896.html (quoting NSA chief Gen. Keith Alexander as saying that there should be some way to stop journalists "giving . . . out" NSA documents leaked by Edward Snowden).

150. Such as, for example, the obligation of lawyers to protect client confidences, *see* MODEL CODE OF PROF'L CONDUCT R. 1.6 (1999), or doctor-patient confidences, backed by HIPPA. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in sections 18, 26, 29, 42 U.S.C (2000)).

151. *"The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century": Hearing on H.R. 2471 Before the Subcomm. On Privacy, Tech. & the Law of the S. Comm. On the Judiciary*, 112th Cong. (2012); California Anti-Paparazzi Statute, CAL. CIV. CODE § 1708.8 (West 2015); New Jersey Anti-Revenge Porn Statute, N.J. STAT. ANN. § 2C:14-9 (West 2004).

152. *See* Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1161 (2005).

153. *Cf.* Part IV.A (discussing to what extent there is a First Amendment right to data collection as well as data sharing).

154. The private sphere is that part of life where individuals have traditionally had the most autonomy, such as the family and the home. *See* JURGEN HABERMAS, THE STRUCTURAL TRANSFORMATION OF THE PUBLIC SPHERE: AN INQUIRY INTO A CATEGORY OF BOURGEOIS SOCIETY (trans. Thomas Burger, 1989).

155. The monitoring may be by the cell phone service provider or by a third party. If the monitoring is by the cell phone provider, and if it was disclosed in the initial contract with the end-user, then it differs from the other cases on this list in that it may be a consequence of a contract and thus may not be as easily modeled as an externality.

156. *See* Kirill Levashov, Note, *The Rise Of A New Type Of Surveillance For Which The Law Wasn't Ready*, 15 COLUM. SCI. & TECH. L. REV. 164 (2013).

157. Bryce Clayton Newell, *Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information*, 66 ME. L. REV. 398, 399 (2014).

(2) Sensors aimed at private property from public locations. This category would include situations like those in *Kyllo*, and;

(3) The closely related case of sensors located on private property that traverse a public area in order to collect information from other private property.[158] For example, a camera on a private building aimed at apartments in the building across the street is no different for these purposes from a camera set up on a public space.

As with physical pollution, in each of these three cases of privacy pollution the data-collector imposes an externality on the data subject.[159] As with physical pollution, constitutional and common law remedies rarely have meaningful traction, whether due to legal or economic constraints. It can be hard to find the sources of most physical pollution unless it is very close or very vivid; similarly, we often do not know the sources of privacy pollution because we do not know who is collecting information about us. Indeed, the fate of privacy in public places shares some features with the tragedy of the commons.[160] There are no relevant ownership rights to the information about what one does in public.[161] A personal datum has value to the subject, who might wish to control it by keeping it private and/or controlling its release. That datum also has value to a whole host of public and private actors who would like access to it for objectives ranging from public safety to modeling group behavior to targeted marketing.

One arguable difference, however, between physical and privacy pollution deserves mention. Exposure to a given amount of a particular chemical over the course of a day causes an equal likelihood of damage whatever its source.[162] It could be argued that not all surveillance is equal, since much of the damage is caused by how the data is used, and that use happens well after the time of collection. In this view, mere collection without use will, in many cases, cause no harm at all. Yet for many, the knowledge that one is being observed and recorded—or even that there is a substantial likelihood of being surveilled—is itself a harm that not only chills speech,[163] but generally inhibits freedom and self-realization.[164]

---

158. This excludes surveillance that takes place entirely on private property (for example a surveillance camera in a home or in an office that is not usually open to the public).

159. Swire & Litan, *supra* note 79, at 5.

160. The parallel is imperfect, because in the classic commons problem each actor faces personal incentives that are collectively harmful, but with sensor deployment, even though many of us have cell phones and thus may contribute to the privacy problems, actors deploying mass sensors have a disproportionate role in privacy-destruction; the rest of us are primarily victims. *See supra* text accompanying notes 87–92.

161. A provider may claim ownership of a virtual public space, such as Twitter or Facebook, but the service's nature means that provider's interest is in making user content accessible to more people rather than trying to write acceptable use policies that limit reuse which could be harmful to people by making their information widely visible.

162. *Environment and Health Risks: A Review of the Influence and Effects of Social Inequalities*, WORLD HEALTH ORG. 5 (2010), *available at* http://www.euro.who.int/__data/assets/pdf_file/0003/78069/E93670.pdf.

163. *See* Emily Bell et al., *Comment to Review Group on Intelligence and Communications Technologies Regarding the Effects of Mass Surveillance on the Practice of Journalism* 1 (Oct. 4, 2013), http://towcenter.org/wp-content/uploads/2013/10/Letter-Effect-of-mass-surveillance-on-journalism.pdf.

Similarly, views may differ as to the relative harmfulness of different types of surveillance. All molecules of a toxic chemical may be alike, but one could argue that governmental surveillance for national security or law enforcement purposes is different from private data collection for profit, fun, or academic purposes. While the general issue of privacy harms is beyond the scope of this Article,[165] for present purposes it suffices to say that this objection seems more like a cost-benefit debate over how much pollution should be tolerated for given economic or other benefits rather than a challenge to the basic idea that privacy pollution is an externality imposed by some on others.

The systematic collection of personal data is a big and urgent problem, and the pace of that collection is accelerating as the cost of collection plummets.[166] Worse, the continued development of data processing technology means that this data can be used and cross-indexed increasingly effectively and cheaply.[167] Add in the fact that there is more and more historical data, as well as self-reported data,[168] to which the sensor data can be linked, and we will soon find ourselves in the equivalent of a digital goldfish bowl. The problem is acute in the private and public sectors, although it is difficult to know the true scope in either case since this information is difficult to acquire.

---

164. *See* JULIE COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE AND THE PLAY OF EVERYDAY PRACTICE (2012); Kaminsky & Witnov, *supra* note 5; Neil Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008).

165. For discussions see e.g., Julie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904 (2013); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011); Daniel J. Solove, *"I've Got Nothing To Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007).

166. *See A History of Storage Cost (Update)*, KMOMO.COM, http://www.mkomo.com/cost-per-gigabyte-update (showing steep decline in cost per gigabyte of storage between 1980 and 2015) (last updated Mar. 9, 2014).

167. This follows from the expanded version of Moore's Law. *See* Annie Sneed, *Moore's Law Keeps Going, Defying Expectations*, SCI. AM. (May 19, 2015), http://www.scientificamerican.com/article/moore-s-law-keeps-going-defying-expectations/.

168. *See generally* Jerry Kang et al., *Self-Surveillance Privacy*, 97 IOWA L. REV. 809, 825 (2012) (observing that a large portion of surveillance is "self surveillance"); Alessandro Acquisti et al., *Faces of Facebook: Privacy in the Age of Augmented Reality*, FACE RECOGNITION STUDY- FAQ, http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/ (discussing research demonstrating ease of linking real-time photographs to Facebook identities); Om Malik, *Why Facebook Home Bothers Me: It Destroys Any Notion of Privacy*, GIGAOM.COM (Apr. 4, 2013, 12:50 PM), http://gigaom.com/2013/04/04/why-facebook-home-bothers-me-it-destroys-any-notion-of-privacy/.
Between 41% and 50% of tweets are about the authors themselves rather than other persons or things. Lee Humphreys et al., *How much is too much? Privacy Issues on Twitter. Conference of International Communication Association, Singapore*, 1, 6 (2010), *available at* http://www3.cs.stonybrook.edu/~phillipa/papers/ica10.pdf. However, only a very small fraction of tweets relays personally identifiable information to the reader. *Id.* at 16. But this fraction still amounts to 360,000 tweets per day that may share location and time information of the author. *Id.* Twitter reports 200 million active users as of March, 2013, with 400 million tweets each day. Karen Wickre, *Celebrating #Twitter7*, TWITTER BLOG (Mar. 21, 2013, 7:42 AM), https://blog.twitter.com/2013/celebrating-twitter7 (however, it is unclear whether those active users are monthly or daily). Facebook reported 1.19 billion monthly active users and 728 million daily active users as of September, 2013. *Facebook Reports Third Quarter 2013 Results*, PRNEWSWIRE.COM (Oct. 30, 2013), http://www.prnewswire.com/news-releases/facebook-reports-third-quarter-2013-results-229923821.html. Instagram reports 300 million active monthly users with 70 million average postings per day. *Our Story*, INSTAGRAM, http://instagram.com/press/# (last visited Apr. 3, 2015).

This last point—our ignorance about the extent of mass surveillance and of its costs—bears emphasis. It should be added that we are also not fully informed about the likely benefits of mass surveillance. That lack will, however, more than likely solve itself because private and public entities are and will be highly incentivized—whether by profit, altruism, or fear—to extract and trumpet as many of those benefits as they can.[169] At present, however, we are not well placed to attempt cost-benefit analysis. Against these known and future benefits we can at present put only poorly understood costs—costs that are more likely to be qualitative than easily monetized.[170] Left to themselves therefore, both the market and the post-9/11 pressures in the name of public safety will tend strongly towards mass surveillance.[171]

III. LEARNING FROM NATIONAL ENVIRONMENTAL PROTECTION ACT

It is certainly time, or perhaps even past time, to do something. I suggest we borrow home-grown solutions from U.S. environmental law. By combining the best features of a number of existing environmental laws and regulations, and—not least—by learning from some of their mistakes, we can craft rules mandating notices and disclosures about data collection practices that would go some significant distance towards stemming the tide of potentially privacy-harming technologies being, and about to be, deployed.

This is why I propose that we require Privacy Impact Notices ("PINs")[172] before allowing large public or private projects that risk having a significant[173] impact on personal information privacy or on privacy in public. The PINs requirement would be modeled on existing environmental laws, most notably the National Environmental Policy Act of 1969 ("NEPA"),[174] the law that called into being the Environmental Impact Statement ("EIS"). It would also take advantage of progress in eco-

169. Some of the advocates may be unexpected. Consider Jane Stanley, *Police Body-Mounted Cameras: With Right Policies in Place, a Win For All*, AMERICAN CIVIL LIBERTIES UNION (Oct. 9, 2013), https://www.aclu.org/technology-and-liberty/police-body-mounted-cameras-right-policies-place-win-all (praising the use of police body-mounted cameras to record audio and video of the officer's interactions with the public but noting significant privacy challenges). The call for body-mounted cameras on police has only intensified after the shooting of Michael Brown in Ferguson, MO. *See, e.g.*, Alan Gomez, *After Ferguson, Police Rush to buy Body Cameras*, USA TODAY (Oct. 11, 2014, 3:22 PM), http://www.usatoday.com/story/news/nation/2014/10/11/police-body-cameras-ferguson-privacy-concerns/16587679/.

170. *See* Peter Swire, *Efficient Confidentiality for Privacy, Security and Confidential Business Information*, Brookings Papers on Economic Activity (forthcoming 2015), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=398340.

171. My colleague Felix Mormann suggests that if the pollution analogy is unsatisfactory, one might think of surveillance as resembling resource extraction, where the resource is privacy. In that scenario we do not live in a privacy goldfish bowl, but rather in an information ocean subject to drift-net fishing. *But see supra* note 92 (suggesting a limit to the extraction analogy).

172. "Privacy Impact Statements" would make for better parallelism with Environmental Impact Statements but the plural form of the resulting acronym would be unfortunate. PINs could also stand for "Privacy Invasion Notices" in order to make them more attention-getting.

173. This is of course the critical word, both in the NEPA context and here.

174. *See supra* note 2.

system modeling, particularly the insight that complex systems like ecologies, whether of living things or the data about them, are dynamic systems that must be re-sampled over time in order to understand how they are changing and whether mitigation measures or legal protections are working.[175]

The overarching goals of this regulatory scheme are familiar from environmental law and policy-making: to inform the public of decisions being considered (or made) that affect it, to solicit public feedback as plans are designed, and to encourage decision-makers to consider privacy and public opinion from an early stage in their design and approval processes. That was NEPA's goal,[176] however imperfectly achieved. In addition, we now know from the environmental law and policy experience that it is also important to invest effort in on-going, or at least annual, reporting requirements in order to allow the periodic re-appraisal of the legitimacy and net social utility of the regulated activity. This is especially true for data collection programs because surveillance technologies change quickly, and because the accumulation of personal information by those gathering data can have unexpected synergistic effects as we learn new ways of linking previously disparate data sets.

PINs differ from existing U.S. rules requiring Privacy Impact Assessments ("PIA"s). At present the E-Government Act requires that federal agencies conduct internal PIAs only for certain projects undertaken by federal agencies.[177] PINs would reach much further, ideally including state or local projects, and even private projects.[178] Second, as further discussed below,[179] neither voluntary private PIAs nor mandatory public PIAs create a right to demand correction, no matter how inept or inaccurate the PIA may be—much less create a right to change or delay the course of the project that triggered the report on the grounds that the disclosures are inadequate. Like Environmental Impact Statements, PINs would do both when triggered by incomplete disclosure. While the underlying analysis contained in a PIN is basically a careful PIA, the legal environment will be very different. Thus, while the world hardly needs another acronym, it seems useful to signal in some very direct way that a PIN could have legal consequences for its drafters in a way that PIAs as currently practiced in the United States do not.

---

175. *See* U.S. ENVIRONMENTAL PROTECTION AGENCY, OFFICE OF FEDERAL ACTIVITIES, *CONSIDERING ECOLOGICAL PROCESSES IN ENVIRONMENTAL IMPACT ASSESSMENTS* (July 1999), http://www.epa.gov/oecaerth/resources/policies/nepa/ecological-processes-eia-pg.pdf; Julie Thrower, Comment, *Adaptive Management and NEPA: How a Nonequilibrium View of Ecosystems Mandates Flexible Regulation*, 33 ECOLOGY L.Q. 871 (2006).

176. *Basic Information*, NATIONAL ENVIRONMENTAL POLICY ACT, http://www.epa.gov/compliance/basics/nepa.html (last updated June 25, 2012).

177. E-Government Act of 2002, Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921–22 (2002).

178. There may be some federalism constraints on the power of Congress to impose permitting requirements on some state/local projects. To the extent that state agencies might be required to impose the PINs, there might also be commandeering issues that NEPA avoids by conditioning its applicability to federal permits or funding.

179. *See infra* text at notes 245–49.

The PINs proposal intersects with active and on-going debates over the value of notice policies.[180] Currently, the major existing notice-based rules designed to protect privacy are after-the-fact state[181] and federal[182] data breach notification requirements. (Before we had modern water pollution law, we had tort liability for dam breaches.[183] In this too, perhaps, the evolution of privacy law will parallel environmental law.)

Although they would have a few teeth, as a regime of notice rather than prohibition PINs would provide less privacy protection than is found in European-style data protection rules. PINs are also more limited than European proposals to adopt an assessment process that would consider practices and technologies in the context of the broader societal impacts of surveillance on society.[184] Unlike the Surveillance Assessments being discussed in the EU, PINs would be focused solely on the consequences to personal privacy. Indeed, the PINs proposal is in many ways weaker than European privacy-protection proposals embedded in the revised European Privacy Regulation.[185]

Proponents of European-style privacy regulation will see the PINs proposal as weak tea. Given current U.S. political and regulatory realities this is a virtue as much as a vice. The PINs proposal is self-consciously tailored to U.S. political and regulatory realities in three significant ways. First, it recognizes that U.S. regulation has consistently rejected European approaches to data protection. Second, by recasting privacy harms as a form of pollution and invoking a familiar (if not entirely uncontroversial) domestic regulatory solution either directly or by analogy, the PINs proposal seeks to present a domesticated form of regulation with the potential to ignite a regulatory dynamic by collecting information about the privacy costs of previously unregulated activities that should, in the end, lead to significant results without running afoul of po-

180. *See infra* Part IV.C. It also builds on, but in at least one critical way diverges from, the work of Dennis D. Hirsch, who in 2006 had the important insight—even truer today—that many privacy problems resemble pollution problems and that therefore privacy-protective regulation could profitably be based on the latest learning from environmental law. *See* Hirsch, *supra* note 79.

181. *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 913 (2006) (advocating for the "[c]reation of a coordinated response architecture" rather than "[m]itigating the harm after a data leak").

182. For a compilation of state data breach laws, see Mintz Levin, *State Data Security Breach Notification Laws*, http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf (current as of Jan. 1, 2015). *See also* A. Michael Froomkin, *Government Data Breaches*, 24 BERKELEY TECH L. J. 1019 (2009) (discussing data breach rules applying to governmental bodies).

183. *See, e.g.*, Rylands v. Fletcher, [1868] UKHL 1.

184. *See* David Wright & Charles D. Raab, *Constructing a Surveillance Impact Assessment*, 28 COMP. L. & SEC. REV. 613, 614 (2012); *see also Final Report: Findings and Recommedations*, SAPIENT, http://www.sapientproject.eu/D5.3%20-%20Final%20report%20(submitted%2004%20September%202014).pdf.

185. Although discussions were still in progress as this Article went to press, the EU seems likely to approve a substantially revised General Privacy Regulation late in 2015. *See* John Bowman, *After Hard DAPIX Work, GDPR Stage Is Set*, PRIVACY PERSPECTIVES (May 21, 2015), https://privacyassociation.org/news/a/dapix-concludes-gdpr-discussions-ahead-of-june-council/. A draft text—"Unofficial consolidated version GDPR"—can be found at http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf.

tential U.S. constitutional limits that may constrain data retention and use policies. Third, for better or worse it adopts the U.S. frame that, politically, it is not enough to assert that privacy is a fundamental right and thus deserving of protections. Rather, potentially costly new privacy-protecting rules need to be in most cases tightly coupled with analyses demonstrating that the rules will create benefits (often monetizable) that justify the costs.[186] We do not at present have those data; a PINs regime presents one means of stimulating the private and public sectors to create mechanisms by which we can get them.

Within the United States, at present the most advanced data-collection operation appears to be the increasingly public multi-faceted domestic surveillance operation conducted by the National Security Agency ("NSA").[187] It is very important to understand the full contours of the still-unraveling secret spy project and to bring it under control, but it is also important to keep track of other developments that also promise to collect and collate far more varied and detailed data about nearly everyone's lives. When it comes to personal data there are three parallel types of collection in action or in formation: the national security sector (the NSA and other intelligence-gathering bodies), civilian governmental agencies, and the private sector.[188] Although they are not totally distinct since they share data, their legal basis and purposes are distinct. The PIN proposal set out in this Article could apply to each, or to all.[189]

This Article's primary goal, however, is to suggest that the PIN solution has value for the problem of data collection in or through public spaces. The Sections that follow make the case that although nowhere near a complete solution to the problem of surveillance even in its broadest application, requiring PINs would contribute significantly to personal information privacy and would do so without running into most of the constitutional and other roadblocks that may have held back attempts to craft more comprehensive European-style regulatory strategies. For now, put aside the NSA and issues of virtual surveillance of Internet and telephone data; these will return in Part III.F below.

A. Privacy Impact Notices (PINs) As a Practical Solution

If we do not trust institutions embarking on massive monitoring programs to monitor themselves—and nothing in history or human nature suggests that we should—then that monitoring needs to come from

186. *See* Jack Beermann, *Safe at Any Speed: Robert Ahdieh's Take on Cost-Benefit Analysis in Financial Markets*, JOTWELL (Nov. 26, 2014) (reviewing Robert B. Ahdieh, I, 88 N.Y.U.L. Rev. 1983 (2013)), http://adlaw.jotwell.com/safe-at-any-speed-robert-ahdiehs-take-on-cost-benefit-analysis-in-financial-markets/ (identifying the values advanced by cost-benefit analysis as including enhancing efficiency, reducing cognitive bias, forcing rational priority setting, reducing regulation, and increasing transparency through clearer analysis and enhanced monitoring of agencies).

187. *See infra* Part III.F.

188. *See infra* Part III.D.

189. Issues of scope are discussed further *infra* Part III.D.3.

somewhere else. The government can do the monitoring directly,[190] or it can attempt to repair some of the deficits that make private action unlikely or impossible. To the extent that the privacy problems are the result of market failure, I am not optimistic about the ability of market-based regulation to cause parties to internalize the externalities nor to overcome the transactions-cost based problems that make markets unlikely to be effective.[191] Thus, some old-style regulation may be needed.

Well-crafted regulation will provide the public with access to the information necessary to inform themselves as to how much personal privacy is being reduced. Making that information available before major projects with significant privacy consequences go forward can inject an element of public deliberation—and perhaps a little caution or search for mitigation—into the decisions to deploy sensors on a large scale. A requirement that some projects produce PINs before being allowed to deploy sensors is one possible model. To regulate with as effective and as light a hand as possible will require fairly detailed information about what personally identifiable information ("PII") is being collected and how it will be linked to other data, which is where an updated NEPA model comes into play.

B. How Environmental Impact Statements Work

NEPA requires Environmental Impact Statements ("EISs") only as the culmination of a series of decisions. The number of projects annually required to file EISs is actually quite small because, as we will see, the proponents of most projects are able to structure their projects, or craft their initial project documentation, in a way that avoids an EIS requirement. As will be argued below, this reflects both strengths and weaknesses of the EIS system.

NEPA is the classic piece of "action-forcing legislation." NEPA requires that an EIS be "included in every recommendation or report on proposals for legislation and other major Federal actions significantly affecting the quality of the human environment."[192] This duty falls on the federal agency controlling the project.[193] Some agencies prepare their own EISs,[194] particularly for projects they initiate. Other agencies farm out the job to the private proponent of a project, particularly if the agen-

190. The challenge is to do so with the minimum amount of command-and-control rules possible. *See infra* text accompanying notes 222–26.

191. I say this despite some inventive suggestions in the literature, *e.g.* Ian Ayres & Matthew Funk, *Marketing Privacy*, 20 YALE J. ON REG. 77 (2003) (suggesting rule requiring telemarketers and phone surveys to compensate consumers for taking their calls with prices based on per-minute charges each of the consumers would set at centralized database online). In general, due to the transaction costs involved, market solutions will rarely work to combat mass surveillance.

192. National Environmental Policy Act of 1969, Pub. L. No.91-190, § 102(2)(C), 83 Stat. 852 (codified at 42 U.S.C. § 4332(2)(C) (2012)).

193. *Id.*

194. The specialization and complexity of the work often leads to sending the work out to consultants.

cy's role is licensing rather than project management,[195] but the agency retains the burden of defending the EIS in court as long as the agency judges the EIS to be sufficient.[196] NEPA also established the President's Council on Environmental Quality ("CEQ"), an agency in the Executive Office of the President that oversees federal agency implementation of the environmental assessment process and advises the president on environmental issues.[197]

In theory, NEPA applies to any environmentally significant project that requires a federal permit, has federal government funding, or takes place on or affects federal land, excluding projects directly legislated by Congress.[198] In practice, however, there are many ways that projects subject to NEPA escape the EIS requirement due to the fact that the route to an EIS has four distinct stages, which are outlined below.

1. *Determine Coverage.* Determine whether the project even needs to be analyzed at all. Projects subject to "functional equivalent" regulations that require a comparable environmental analysis are excluded from NEPA.[199]

2. *Categorical Exclusions.* Determine whether any blanket waivers, called "Categorical Exclusions" ("CE"s),[200] apply. CEs are regulatory decisions by an agency with appropriate jurisdiction that a class of activities does not individually or cumulatively have a significant effect on the quality of the human environment.[201] Agencies issue CEs through the standard informal rulemaking process, which means that they publish a draft in the Federal Register for public comment, and then publish a final draft together with the agency's responses to the comments.[202] Once the CE is final, the class of covered activities will only trigger an EIS if the agency finds the project involves extraordinary circumstances—for example, the extinction of a species. If extraordinary circumstances apply, or the activity is not covered by a CE, then the agency must go on to the next step, and must prepare an Environmental Assessment ("EA").[203]

---

195. For example, the Atomic Energy Commission used to require applicants for authorization to operate nuclear power plants to prepare the EIS for the project. *See, e.g.*, Calvert Cliffs' Coordinating Comm. v. U.S. Atomic Energy Comm'n, 449 F.2d 1109 (D.C. Cir. 1971) (requiring the AEC to follow Congress' mandate and require environmental notices before projects are approved). The Atomic Energy Commission was replaced by the U.S. Nuclear Regulatory Commission in 1974. *See AEC to NRC*, U.S. NUCLEAR REG. COMMISSION, http://www.nrc.gov/about-nrc/history.html (last updated Sept. 30, 2014).

196. *See, e.g.*, *Calvert Cliffs' Coordinating Comm.*, 449 F.2d at 1109 (requiring AEC to defend its EIS).

197. *See Council on Environmental Quality - About*, WHITE HOUSE, http://www.whitehouse.gov/administration/eop/ceq/about (last visited Apr. 3, 2015).

198. National Environmental Policy Act § 102(2)(C) (codified at 42 U.S.C. § 4332(2)(C)).

199. *See* CAL. PUB. RES. CODE § 21080.5 (West 2014); *see also* Portland Cement Ass'n v. Ruckelshaus, 486 F.2d 375, 384–85 (D.C. Cir. 1973) (articulating the functional equivalence standard).

200. *See* 23 C.F.R. § 771.117(a) (2014); *NEPA Documentation,* DOT.GOV, http://www.environment.fhwa.dot.gov/projdev/pd4document.asp (last visited Apr. 3, 2015).

201. *See* 40 C.F.R. § 1508.4 (2014).

202. *Id.* § 1503.

203. *See id.* § 1508.4.

3. *Environmental Assessment.* If no CEs apply, ordinarily the next step in the permitting or approval process is deciding whether the environmental impact of the proposed activity is "significant."[204] The federal agency controlling the project produces[205] an Environmental Assessment ("EA"), which is a determination of the environmental effects of the proposal and a survey of possible alternative means.[206] Armed with this preliminary analysis, the agency either requires a full-dress EIS or issues a Finding of No Significant Impact ("FONSI") on the environment.[207] Unless someone challenges the FONSI as wrongly granted, a FONSI is the end of the road under NEPA; indeed, a very large number of proposals stop there.[208]

4. *Environmental Impact Statement ("EIS").* In the absence of a CE or a FONSI, any project within NEPA's scope must proceed to the preparation of a full EIS.[209] An EIS is a much more involved procedure than an EA; the public, interested parties, and other agencies, are all able to comment on the draft EIS. NEPA requires that an EIS include "a detailed statement by the responsible official on:"

(i) the environmental impact of the proposed action;

(ii) any adverse environmental effects which cannot be avoided should the proposal be implemented;

(iii) alternatives to the proposed action;

(iv) the relationship between local short-term uses of man's [*sic*] environment and the maintenance and enhancement of long-term productivity; and

(v) any irreversible and irretrievable commitments of resources which would be involved in the proposed action should it be implemented.[210]

NEPA does not create criminal or civil sanctions. Instead, plaintiffs have the right to complain in federal court that the EIS is incomplete or inadequate.[211] The remedy for a successful suit is an order to rethink the project or the permit approval, which involves redoing the EIS.[212] Such an order usually causes extensive delay to the project.

---

204. *See id.* § 1508.9.

205. There is a slightly fictional cast to this account in that, especially in permitting matters, the private party with an interest in having the project go forward commonly will do the heavy lifting on the drafting.

206. If there's no doubt about the scope of the environmental harm, the agency has the option of skipping the EA and going straight to the EIS.

207. *See* 40 C.F.R. § 1508.9 (2014).

208. Albert I. Herson, *Project Mitigation Revisited: Most Courts Approve Findings of No Significant Impact Justified by Mitigation*, 13 ECOLOGY L.Q. 51 (1986).

209. *See* National Environmental Policy Act of 1969, Pub. L. No. 91-190, § 102(2)(C), 83 Stat. 852 (codified at 42 U.S.C. § 4332(2)(C) (2012)).

210. *Id.* § 102(2).

211. *See* 40 C.F.R. § 1508.18.

212. *See* Bradley C. Karkkainen, *Toward a Smarter NEPA: Monitoring and Managing Government's Environmental Performance*, 102 COLUM. L. REV. 903, 917–18 (2002).

Given the great number of projects that make it to the EA stage, the federal government actually requires remarkably few EISs every year, perhaps one in one hundred.[213] The vast majority get FONSIs, either because their environmental impact is genuinely low, or because the project's proponents promise sufficient mitigation efforts to allow the agency to find that the net environmental impact will not be "significant."[214] These so-called "mitigated FONSIs" have been criticized as an institutionalized end-run around the EIS requirements,[215] but they have also been praised as a sign that the EIS regime is actually working remarkably well; fearing the costs and delays that a full EIS can cause, project proponents have chosen to promise to reduce the environmental costs of their proposals right from the design stage.[216] If this is actually what is happening—if the mitigation is more than a paper tiger—then NEPA's 'action forcing' mechanism is a real success.

Unfortunately, there is not enough systematic follow up of the environmental effects of projects approved with mitigated FONSIs, much less an organized assessment of whether the mitigation was effective; in many cases, we do not even know if the mitigation turned out to be anything more than a promise.[217] Any adoption of the EIS regime to the privacy context thus must include follow up reporting requirements in order for the administering agency to be able to determine how the privacy consequences of the project compared to those predicted, and also to allow it to evaluate the effectiveness (not to mention the actual existence) of any mitigation strategies that the agency relied on in issuing a privacy FONSI.

C. *PINs as Improved EISs*

Suitably modified and updated, the EIS could be a good model for PINs.[218] By requiring public notice of large and continuing data collection efforts that will collect personally identifiable information in public or online, and by creating a right of action in cases where those disclosures are inadequate, a PIN requirement would ensure that public and private bodies thinking of deploying covered potentially privacy-harming technologies would have greater incentives to build in privacy protections—Privacy by Design[219]—or look for alternate means to achieve their goals.

---

213. *See id.* at 909–10.

214. *Id.* at 909–10.

215. *See* Donald McGillivray, *Mitigation and Screening for Environmental Assessment*, 12 J. PLANNING & ENVTL. L. 1539, 1552 (arguing that mitigated FONSIs are inherently suspect).

216. *See* Karkkainen, *supra* note 212, at 909–10.

217. *See id.* at 927.

218. Blair Stewart, New Zealand's Assistant Privacy Commissioner, may have been the first to note the similarities between PIAs and EISs. *See* Blair Stewart, *Privacy Impact Assessments*, 3 PRIVACY L. & POL'Y REP. 39 (1996); Blair Stewart, *PIAs—an Early Warning System*, 3 PRIVACY L. & POL'Y REP. 65 (1996). I am grateful to Charles Raab for calling my attention to these articles.

219. For an introduction to Privacy By Design, see, for example, Ann Cavoukian, *Privacy by Design and the Emerging Personal Data Ecosystem* (Oct. 31, 2012), http://www.privacybydesign.ca/index.php/paper/privacy-by-design-and-the-emerging-personal-data-ecosystem/; *see generally The Role*

Creating a private right of action in federal court to challenge the adequacy or necessity of the PIN, would ensure that anyone planning to deploy privacy-harming technology fully disclosed (and, one hopes, fully considered) the consequences of their actions.[220]

In his 2006 article on environmental law and privacy, Dennis Hirsch directly rejected what he saw as old-fashioned regulation as a feasible means of dealing with the collection of private data.[221] Instead of the much-maligned command-and-control model of environmental regulation[222] characterized by detailed and inflexible specifications, Hirsch advocated "second generation" rules intended to be more flexible and market-based.[223] These rules give more discretion to the regulated parties, leaving them able to optimize compliance subject to the constraints imposed by performance standards—or sometimes, in the case of co-regulation, what I would characterize as even more-amorphous and less-external constraints.[224]

---

of Privacy by Design in Protecting Consumer Privacy, CTR. FOR DEMOCRACY AND TECH. (Jan. 28, 2010), https://www.cdt.org/policy/role-privacy-design-protecting-consumer-privacy.

220. I recognize that this is a tall order: private rights of action are not in favor in Congress or the courts at present. In particular, the Supreme Court has been increasingly clear that it will not imply private rights of action; the right must be explicit in a statute for it to be enforceable. *See* Alexander v. Sandoval, 532 U.S. 275, 286–87 (2001); *see also* Gonzaga Univ. v. Doe, 536 U.S. 273, 273 (2002) (foreclosing a suit brought by student trying to enforce provisions of the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232(g)); Cannon v. Univ. of Chi., 441 U.S. 677, 718 (1979) (Rehnquist, J., concurring) ("This Court . . . should be extremely reluctant to imply a cause of action absent such specificity on the part of the Legislative Branch.").

221. Hirsch, *supra* note 79, at 59–60 (arguing for a "second generation approach that takes advantage of firms' ability to redesign their own operations").

222. *See* Richard B. Stewart, *A New Generation of Environmental Regulation?*, 29 CAP. U. L. REV. 21 (2001) (comparing "first" and "second" generations of environmental regulation); Richard B. Stewart, *The Reformation of American Administrative Law*, 88 HARV. L. REV. 1669. 1669 (1975) (tracing the "fundamental transformation that calls into question its [referring to administrative law] appropriate role in our legal system"). Hirsch agrees (as do I) with these classic accounts' conclusion that one of the errors of much early environmental regulation was a focus on specific technologies and specific duties. Hirsch, *supra* note 79, at 59–60; *see also* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 303 (2011) ("The shortcomings of command-and-control governance . . . are well recognized."). *But see* Jodi L. Short, *The Paranoid Style in Regulatory Reform*, 63 HASTINGS L.J. 633, 638 (2012) (noting "the prevalence of state-coercion arguments within regulatory reform discourse, the rise of self-regulation from within this same discourse, and the connection between the two").

223. One of Hirsch's other main suggestions, based on "second generation" rulemaking, was that we should seek to achieve privacy goals via regulatory covenants modeled on environmental covenants. These covenants are contracts negotiated between a regulator and the subject of the rule, usually with other interested parties also participating. Hirsch, *supra* note 79, at 41–43, 50–57. Experience suggests, however, that this type of negotiation is not just ineffective, but may actually be counterproductive. *See* Cary Coglianese, *Assessing Consensus: The Promise and Performance of Negotiated Rulemaking*, 46 DUKE L.J. 1255, 1261 (1997) (reporting that negotiated rulemaking failed to provide promised benefits of decreased litigation and expeditious rulemaking; indeed, evidence from EPA suggested litigation rates increased). Hirsch also suggested that we should use the model of emissions fees to control spam, which is made possible by the low marginal cost of email. *See supra* note 79, at 40–50.

224. For an argument in favor of co-regulatory strategies, see Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. REV. 1, 2 (1997). Hirsch endorses co-regulation strategies in Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439, 441 (2011).

In principle, I agree that we should have a presumption in favor of market-based solutions and avoid command-and-control regulation whenever possible. In cases where we can design good self-policing mechanisms,[225] or even solutions in which an external party has an incentive to act as the monitor,[226] market-based solutions should tend to be much more efficient than mandating compliance with an inflexible technology standard. In contrast, even with the best will in the world, technology standards administered by bureaucrats will tend to lag market-based responses. That debate, however, is at present largely inapposite to the problem of regulation of privacy-harming technologies and practices. Even if harm to privacy can at a general level usefully be analogized to harm to the physical environment, privacy remains more difficult to meter than physical pollutants.[227] There is no standard unit of privacy to allow any sort of comparison between intrusions, and privacy is notoriously difficult to monetize, making invocation of the economists' universal comparative, the dollar, even more difficult than usual. Similarly, there are at present no broad-spectrum technologies that one would want to prescribe to preserve individual privacy.[228] Rather, the major tools in the privacy arsenal are limits on over-intrusive data collection, and limits on information re-use beyond the purposes for which it was collected. Some data-collection mechanisms, however, can be degraded at source (e.g.

225. This is a key caveat, as without it too much "second generation" or "third way" regulation ends up with the foxes regulating the chicken coop with an inter-species committee containing a token chicken.

226. The classic example is an insurance requirement, in which we somewhat optimistically rely on the insurers to monitor risk and set prices accordingly.

227. In comments on an earlier draft, Dennis Hirsch suggested that privacy violations are no harder to monitor than pollution because "[t]he number of data points released through a data breach is just as amenable to quantification as is the amount of pollution released through a smokestack," as are the number of data points on each individual, number of individuals in the database, and the number of transfers of this data to third-parties. E-mail from Dennis Hirsch to author (June 3, 2013) (on file with author).

I disagree for two sets of reasons. First, pollution can be monitored externally, e.g. from water or air samples. Only some data collection is externally visible, and none of the collation or storage is externally visible. Even when data releases are externally visible, they will often be harder to trace than a toxic spill or a smokestack emission: it often will neither be clear which third parties have accessed the data nor how they may have reused it. Second, even when data-collection violations can be detected, the value of the harm is harder to monetize. Admittedly, the monetization of environmental harms is itself something of a black art, but there is now a large body of experience in which we attempt to measure the health costs of pollution, Press Release, European Env't Agency, *Reducing the € 45 Billion Health Cost of Air Pollution from Lorries* (Feb. 28, 2013) http://www.eea.europa.eu/pressroom/newsreleases/reducing-the-20ac-45-billion (last visited Apr. 3, 2015), and the costs of clean-up. *See Cleaning Up Nigerian Oil Pollution Could Take 30 Years, Cost Billions – UN*, UN NEWS CENTRE (Aug. 4, 2011), http://www.un.org/apps/news/story.asp?NewsID=39232&Cr=pollutio..#.UcQ_rWig7ll (last visited Apr. 3, 2015). As far as I am aware there is nothing comparable for data collection (or even emission).

228. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010) (discussing weaknesses of de-identification attempts). There are, however, many individually tailored solutions primarily involving the degradation of detail or the extent to which raw information will be kept or just aggregated. For example, sound-monitoring that only captures decibels is superior to recording conversations. Movement tracking that captures locations is problematic, but still superior to capturing actual images; images with faces blurred may be superior to entire images—until gait recognition becomes fully operative.

faces can be blurred in surveillance photos) or raw data can be destroyed after a period of time. These mitigation methods can sometimes be effective, but they tend to be unattractive to the data collector because they either undermine the purposes for which the data is collected or prevent serendipitous uses in light of later discoveries.[229] Our unwillingness to adopt EU-style privacy regulations suggests that these limitations on data re-use, which are essential parts of the EU regulations, are not going to be met with much enthusiasm here either. And short of a very broad-brush ban, it is hard to see how comprehensive regulations modeled on technology standards would have much traction.[230]

Attempting to impose command-and-control rules to deal with privacy problems could be expensive and could risk suppressing innovation.[231] The NEPA-based proposal offered here, however, is not a command-and-control rule, but rather an action-forcing rule.

We are still at such an early stage in the protection of privacy that we do not even have sufficient information about how personal information is being collected, how much is being collected, and how it is being used. We certainly do not have any standardization in how information about personal information collection or use is reported. What is more, information gathering and information processing technologies are changing rapidly, so any information we do learn dates rapidly. Given that it is both legally and practicably difficult to limit the disclosure of information once it is collected, jump-starting a conversation as to whether the information should be collected at all is a necessary part of any strategy designed to create a public conversation about the costs and benefits of pervasive surveillance—a conversation that I take to be the necessary prerequisite to the achievement of any state or national policy with a reasonable hope of protecting personal information privacy.

For all these reasons, I think that NEPA's requirement of EISs—a venerable environmental requirement, contained in legislation that has been called the "Magna Carta of US environmental law"[232]—is a key 'first wave' piece of environmental legislation that, with some updating, could play a useful, perhaps even transformative, role in the regulation of privacy-reducing technologies in public places. NEPA is a good model for two reasons. First, the very thing that sometimes brings it criticism in the environmental context—that NEPA is about forcing the provision of information rather than about direct regulation—could be a strength in the privacy context. Second, the politics of privacy today resembles the politics of environmental law in the late 1960's. Just as public concern

229. These problems are especially acute in the medical data context.

230. The existence of the Fair Credit Reporting Act and the Video Privacy Protection Act suggests that there may be an appetite for regulation in special cases.

231. Hirsch, *supra* note 79, at 34–35.

232. EVA H. HANKS, ET AL., ENVIRONMENTAL LAW AND POLICY: CASES AND MATERIALS xxviii (1974).

about pollution grew following the publication of *Silent Spring*,[233] so now the Snowden revelations about the NSA are causing a national reaction to the surveillance of our movements and communications.[234] Just as NEPA was part of the first-stage response to environmental concerns, a national Privacy Protection Act modeled on it ought to be a politically attractive response to privacy concerns.

NEPA would need to be modernized and adapted to its new context. We have learned a few things about what works and what does not since NEPA was passed in 1969.[235] PINs would not be simply privacy EISs, but rather would need to be privacy EISs version 2.0.

A disclosure/notice regime does not, of course, guarantee any outcome. Rather, it helps create the conditions for a more informed debate by creating more informed citizens and consumers. A disclosure/notice regime may also have economic and competitive effects. If, as I argued above,[236] the market for privacy (or, if you prefer, disclosure) is distorted by consumer myopia, the injection of additional information at a low cost to the individual may at best partially correct the consumer's economic vision. A world of less-myopic consumers may make competition on privacy more attractive as a strategy for some firms that contemplate privacy-enhancing projects; conversely, the specter of mandated disclosure of potentially privacy-harming technology may cause some firms to think twice about their plans if that disclosure were seen as likely to cause bad publicity.[237]

A requirement to conduct even a preliminary privacy assessment—the equivalent of an EA—would serve two other critical functions. First, it would incentivize organizations to consider privacy issues in the early design phase of their projects.[238] Secondly, in the case of projects with potentially significant impacts on privacy, it would form the basis for a conversation with an outside body—the regulator—about which mitigation measures would be appropriate, and what it would take to secure a mitigated FONSI.

---

233. Rachel Carson's *Silent Spring* (1962) is often credited with launching the US environmental movement. RACHEL CARSON, SILENT SPRING (1st ed. 1962); *see, e.g.*, Andrew C. Revkin, *How Rachel Carson Spurred Chemical Concerns by Highlighting Uncertainty*, N.Y. TIMES (Sept. 27, 2012, 7:22 AM), http://dotearth.blogs.nytimes.com/2012/09/27/how-rachel-carson-spurred-chemical-controls-by-highlighting-uncertainty/.

234. *See* Bernie King, *NSA Surveillance Scandal: The Polls Are In, and NSA Spying is Really, Really Unpopular*, POLICYMIC (July 10, 2013), http://mic.com/articles/53767/nsa-surveillance-scandal-the-polls-are-in-and-nsa-spying-is-really-really-unpopular (distinguishing polls that inquired as to surveillance of Americans, as opposed to surveillance in general); Mark Jaycox, *Update: Polls Continue to Show Majority of Americans Against NSA Spying*, EFF (Jan. 22, 2014), https://www.eff.org/deeplinks/2013/10/polls-continue-show-majority-americans-against-nsa-spying (noting polls showing 60% to 74% of Americans object to NSA domestic surveillance).

235. An excellent set of modernizing suggestions are in Karkkainen, *supra* note 212, at 938–48.

236. *See supra* Part II.B.3.

237. *See infra* notes 395–412 and accompanying text.

238. The Office of Management and Budget's rules requiring Privacy Impact Analysis already seek to do this. The PINs rule, with the possibility of judicial review, would up the ante. The requirement would be new for private organizations.

D. Finding the Authority for Privacy Impact Notices (PINs)

Crafting a PIN regime raises two related issues of scope and authority. The most important policy issue is which projects should be covered at all. As described above, NEPA requires EISs for any major federal projects or federally permitted projects "significantly affecting the quality of the human environment."[239] In addition to applying to public projects, NEPA applies to all private projects that require a federal permit.[240] And state "little NEPA" statutes commonly require EISs for broad categories of environmentally significant private actions requiring state approval or receiving state support.[241] In short, NEPA's EIS requirement is triggered either by environmentally significant state action or by permitting, which is a state action prerequisite to certain private actions. The most important practical issue is the legal means by which a PIN requirement could be enacted. As we will see, the widest scope undoubtedly requires fresh legislative authority; arguably, anything but the narrowest scope would also require new legislation.

1. Expand Existing Privacy Impact Assessment (PIA) Requirements

The simplest but narrowest way to enact a limited NEPA-like PIN regime would be to build on existing rules that require federal agencies to consider the privacy consequences of their IT projects. Currently, the Office of Management and Budget ("OMB") requires administrative agencies to conduct PIAs[242] when developing or procuring information technology systems that include personally identifiable information.[243] The OMB rules, which derive from the E-Government Act of 2002,[244] require agencies to do a "risk assessment" to identify and evaluate potential threats to individual privacy, and to identify alternatives and mitiga-

---

239. NEPA, 42 U.S.C. § 4332(2)(C) (2012).

240. Scientists' Inst. for Pub. Info., Inc. v. Atomic Energy Comm'n, 481 F.2d 1079, 1085 (D.C. Cir. 1973) (requiring a detailed EIS for "every recommendation" affecting the quality of human requirement); Calvert Cliffs' Coordinating Comm., Inc. v. U.S. Atomic Energy Comm'n, 449 F.2d 1109, 1111 (D.C. Cir. 1971) (noting that NEPA was designed to cover almost every form of significant federal activity); Gifford-Hill & Co. v. F.T.C., 389 F. Supp. 167, 174 (D.D.C. 1974) (holding that NEPA applies to non-federal projects only if project requires non-ministerial agency action), *aff'd*, 523 F.2d 730, 731 (D.C. Cir. 1975).

241. *See, e.g.*, Minn. Stat. Ann. § 116D.04 (West 2012) (requiring "a detailed environmental impact statement prepared by the responsible government unit" for any "major government action," which is defined as "activities, including projects wholly or partially conducted, permitted, assisted, financed, regulated, or approved by units of government including the federal government.").

242. For a survey of the early literature on PIAs, see Roger Clarke, *Privacy Impact Assessment: Its Origins and Development*, 25 COMPUTER L. & SEC. REV. 123 (2009), *available at* http://www.rogerclarke.com/DV/PIAHist-08.html.

243. *See generally* Kenneth A. Bamberger & Diedre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. CHI. L. REV. 75, 76 (2008) (noting that "[d]ata subject to the immense search and aggregation powers of technology systems, increases the capacity for repurposing and reuse, and provides increasingly attractive targets to hackers bent on misuse. These phenomena raise serious concerns about a surveillance capacity that can erode personal privacy").

244. *See* 44 U.S.C. § 3501 (2012).

tion measures.[245] The proposed PIN system would differ from existing PIAs in that there would be greater opportunity for the public to participate in the creation of the report and, most significantly, the public would have a right to challenge the project if the agency's assessment of the privacy consequences or the feasible alternatives was inadequate. That right is the defining part of NEPA's EIS system, but currently PIAs are not subject to an external check in court.[246] That change will not be popular with agencies, but it will add needed external enforcement to the PIA regime.

As documented by Kenneth A. Bamberger and Diedre K. Mulligan, the quality of federal PIAs varies depending on the quality of agency personnel, their commitment to the enterprise, and the extent to which agency leadership (or the President[247]) treats privacy as a priority.[248] OMB's PIA rules do not create any private rights of action, and thus unless OMB itself goads unwilling agencies there is no check outside the agency, and in any case no check outside the Administration, to ensure PIAs are of even adequate quality. And as Bamberger and Mulligan demonstrate, some clearly are not.[249]

Most likely this approach would require new legislation, as the E-Government Act of 2002 seems unlikely to provide the authority for PINs, and, in any case, certainly does not require PINs.[250] Given its track record, the odds that OMB will voluntarily create a new private right of action against agencies seems infinitesimally low, and its legal authority to do so can also be questioned. Furthermore, the existing PIA regime or any upgraded version of it would only cover projects undertaken directly by federal agencies.

2. *Redefining "Pollution" to Include Destruction of Privacy*

A more direct, but also more controversial, approach would be to add privacy-related factors to the list of things that parties potentially required to complete an EIS have to consider.[251] In other words, we could formally list privacy-destruction as a type of pollution. This addition to the existing NEPA regime could perhaps be achieved without legislation, as the President's Council on Environmental Quality ("CEQ") could amend its regulations.

---

245. *M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, OFFICE OF MGMT. & BUDGET (Sept. 26, 2003), *available at* http://www.whitehouse.gov/omb/memoranda/m03-22.html.

246. *See* Bamberger & Mulligan, *supra* note 243, at 86.

247. Bamberger and Mulligan state that when the Bush administration took office, their appointees de-emphasized privacy and quality suffered. *See id.* at 90.

248. *See generally* Bamberger & Mulligan, *supra* note 222.

249. *See* Bamberger & Mulligan, *supra* note 243, at 90.

250. *See generally* E-Government Act, 44 U.S.C. § 3501 *et seq.* (2012).

251. I am indebted to Richard Williamson for this suggestion.

The argument that the CEQ could simply re-define surveillance as a type of pollution that can trigger an EIS requirement is based on the words of the National Environmental Policy Act of 1969. NEPA speaks in extremely broad terms:

> The Congress authorizes and directs that, *to the fullest extent possible*: (1) the policies, regulations, and public laws of the United States *shall* be interpreted and administered in accordance with the policies set forth in this chapter, and (2) all agencies of the Federal Government shall—
> (A) utilize a *systematic, interdisciplinary* approach which will insure the *integrated use of* the natural and *social sciences* and the environmental design arts in planning and in decisionmaking *[sic]* which *may have an impact on man's [sic] environment*;
> . . .
> (C) include in every recommendation or report on proposals for legislation and other major Federal actions significantly *affecting the quality of the human environment*, a detailed statement by the responsible official on—
> (i) the environmental impact of the proposed action,
> (ii) *any* adverse environmental effects which cannot be avoided should the proposal be implemented,
> (iii) alternatives to the proposed action, . . .[252]

The language is indeed capacious, and it is conceivable that the CEQ could conclude that surveillance, not unlike greenhouse gasses, has an environmental impact within the scope of NEPA. The obvious counter to all this is that despite the capacious language of the statute there is no evidence whatsoever that Congress, in passing NEPA, ever contemplated anything other than the physical harms that we have traditionally understood as pollution.[253] Ironically, the argument for expanding the CEQ's authority to include privacy pollution will primarily appeal to formalist readers of statutes, and rather less to purposivists.

On the other hand, in *Massachusetts v. EPA* the Supreme Court interpreted § 202(a)(1) of the Clean Air Act, which requires the EPA Administrator to regulate "'any air pollutant . . . which in [the EPA Administrator's] judgment cause[s], or contribute[s] to, air pollution . . . reasonably . . . anticipated to endanger public health or welfare'" as requiring EPA to set emission standards for greenhouse gases.[254] If "any air pollutant" that is anticipated "to endanger public health or welfare" includes greenhouse gasses, then why should not the broader language in NEPA be authority for interpreting privacy-harming technology as

252. NEPA, 42 U.S.C. § 4332 (2012) (emphasis added).

253. *See* Metro. Edison Co. v. People Against Nuclear Energy, 460 U.S. 766, 772 (1983) (stating that, in enacting NEPA, Congress was solely concerned with changes in the "physical environment").

254. Massachusetts v. E.P.A., 549 U.S. 497, 528–32 (2007).

something which can "have an impact on man's environment" and indeed risk "significantly affecting the quality of the human environment"?[255] Similarly, the privacy pollution regulation could be distinguished from the FDA tobacco rule struck down in *Brown & Williamson*.[256] In *Brown & Williamson*, the Court's decision that the FDA lacked authority over tobacco products turned on "the unambiguously expressed intent of Congress"[257] because it found that Congress had "clearly precluded the FDA from asserting jurisdiction to regulate tobacco products" and that such authority would be "inconsistent with the intent that Congress has expressed" in subsequent tobacco-specific legislation.[258] The absence of comprehensive federal privacy law means that this argument would be much harder to make against a hypothetical CEQ regulation.

Unfortunately, even in the somewhat unlikely event that the CEQ were willing to redefine mass surveillance as a form of pollution, and the perhaps slightly less unlikely event that the rule were to survive judicial review, many private potentially privacy-harming projects still would not be covered as they do not currently require any sort of permit. Zoning would be one way to reach outdoor sensors; some, mostly state and local, construction permit requirements would be another. Thus, for any PIN requirement to reach many of the greatest threats to personal privacy it will not be enough to rely on existing permitting requirements. We will need something new.

3. *New Legislation*

NEPA (or its substantial equivalent in other statutes) reaches conduct ranging from the construction of nuclear power plants to the disposal of toxic waste to construction projects that threaten wetlands. NEPA owes its relatively broad reach to the large number of statutes that create permitting requirements, whether directly for environmental reasons or to serve other public safety goals.

Privacy regulation today differs from 21st century environmental regulation in one particularly important way: the United States has relatively few data privacy-protective (or privacy-in-public-protective) laws and rules.[259] As described above,[260] NEPA's rules requiring an Environ-

255. 42 U.S.C. § 4332.

256. FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 161 (2000) (holding that the FDA lacked authority to regulate tobacco product marketing).

257. *Id.* at 125–26 (quoting Chevron U.S.A., Inc. v. NRDC Inc., 467 U.S. 837, 842–43 (1984)).

258. FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 126 (2000).

259. *See* Chris Hoofnagle, Directorate-General Justice, Freedom and Security (EC), Comparative Study On Different Approaches to New Privacy Challenges, In Particular In the Light Of Technological Developments: B.1 – United States of America 1 (2010), http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B1_usa.pdf (arguing that "[t]here are no cohesive, core concepts to US privacy law" and that the "US approach is incoherent" and "sectorally-based," with legislative protections being "largely reactive").

260. *See supra* Part III.B.

mental Impact Statement are triggered by state action such as a government project, or a request to issue a permit for private development.[261] No comparable permit requirements exist for mass private data collection. In this, U.S. privacy law today somewhat resembles anti-pollution law before the amendments to the Clean Air Act in 1970[262] and the Clean Water Act of 1972,[263] although this analogy understates the difference since even before the enactment of those laws there were zoning and other rules that could require governmental permission before undertaking private projects.

At present, the United States does not have a national privacy office.[264] The OMB manages compliance with the Privacy Act, a statute which requires federal agencies to publish a Federal Register notice describing the creation of a system of records containing personally identifiable information.[265] President Clinton appointed the first 'Privacy Czar,' Peter Swire,[266] and President Obama has continued the practice of appointing a Chief Privacy Officer ("CPO").[267] Notably, both the OMB and the CPO are in the Executive Office of the President.[268] In addition, many agencies have their own CPOs, some of whom are required by statute.[269]

The environmental law example teaches us that, valuable as these departments and officials may be, these existing bodies would not be enough to administer a PIN regime. Not only does their authority, such as it is, extend only to the conduct of federal officials and in some cases federal contractors, but that authority is somewhat circumscribed. It is unlikely, for example, that (even if they wanted to) either office could transform existing PIAs into full-bore PINs as they lack the authority to create and administer a private notice requirement. Even if the NEPA itself opens the door to classifying privacy as pollution,[270] nothing in the Privacy Act or in the remit of the CPO extends to imposing PINs on pri-

---

261. 42 U.S.C. §§ 4321–47 (2005).

262. First enacted in 1963, the Clean Air Act, Pub. L. No. 88-206, 77 Stat. 392, primarily set up a research program. Modern regulatory controls on air pollution began with the 1970 amendments, the Clean Air Amendments of 1970, Pub. L. No. 91-604, 84 Stat. 1676.

263. Federal Water Pollution Control Act Amendments of 1972, Pub. L. No. 92-500, 86 Stat. 816.

264. Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 SOFTWARE L.J. 199, 202 (1993).

265. UNITED STATES GEN. ACCOUNTING OFFICE, GAO-03-304, *PRIVACY ACT:* OMB LEADERSHIP NEEDED TO IMPROVE AGENCY COMPLIANCE, *available at* http://www.gao.gov/new.items/d033304.pdf.

266. *See* Maria Seminerio, *Clinton to Name Privacy Czar*, ZDNET (Mar. 5, 1999), http://www.zdnet.com/news/clinton-to-name-privacy-czar/101739.

267. *See* Nicole Perlroth, *White House Plans to Add Technology Adviser*, N.Y. TIMES (May 7, 2013, 6:16 PM), http://bits.blogs.nytimes.com/2013/05/07/white-house-plans-to-add-technology-adviser/.

268. *See Office of Management and Budget Open Government Plan*, WHITEHOUSE.GOV (last visited Apr. 3, 2015), http://whitehouse.gov/open/around/eop/omb/plan; *see also* Declan McCullagh, *White House Picks Twitter Lawyer as Internet Privacy Officer*, CNET.COM (May 7, 2013, 10:35 AM), http://news.cnet.com/8301-13578_3-57583249-38/white-house-picks-twitter-lawyer-as-internet-privacy-officer/.

269. *E.g.*, 6 U.S.C. § 222 (2012) (creating the CPO in the Department of Homeland Security).

270. *See supra* Part III.D.2.

vate actors. Note also that the Privacy Act, the key federal law governing the privacy of information held in databases by federal agencies, lacks a meaningful private right of action because privacy harms are so difficult to value. The Supreme Court has held that in order to win relief for violations of the Privacy Act a plaintiff must establish actual damages from the violation.[271]

To fully realize the benefits of PINs will require legislation, and will also require at least one, perhaps two, new administrative bodies. Just as NEPA created the President's Council on Environmental Quality ("CEQ"), the PINs regime would be best achieved by creating a new President's Privacy Council ("PPC")—or an agency headed by a single responsible administrator—with similar powers.[272] If the PINs requirement applied only to federal action, the PPC would have little or no direct responsibility for managing PINs because that would be the responsibility of the lead agency conducting or permitting the project. Thus, for example, a federal agency deploying new systems of sensors or surveillance would take the lead in preparing the PIN, but would be subject to the framework elaborated by the PPC. The agency would also work in the shadow of the threat of a private lawsuit if the PIN was incomplete. At the very least, the PPC would write regulations defining privacy CEs—further defining the activities for which no PINs would be required. Conversely, it might set criteria for mandatory PINs—defining classes of activities that were sufficiently great to automatically trigger a notice requirement. The zone between the CEs and the mandatory PINs would be a greyer area more open to agency discretion, and in particular there could be areas in which the PPC could encourage agencies to experiment with mitigation strategies in the course of issuing mitigation-based FONSIs. The PPC would also serve as a clearinghouse for best practices regarding mitigation strategies that could be incorporated into mitigation-based FONSIs. Furthermore, the PPC would be charged with setting reporting standards, particularly for follow ups designed to measure the extent of privacy harms and the effectiveness of mitigation strategies.[273]

Like the CEQ, the PPC could be part of the Executive Office of the President so long as the PINs reach was limited to potentially privacy-harming projects proposed by the government itself. But if the PINs rule extends to private parties, institutional considerations counsel for a normal, free-standing agency on the model of the EPA—call it the Privacy

271. *See* Doe v. Chao, 540 U.S. 614, 619 (2004) (finding lack of standing despite presence of statutory minimum damages of $1,000 in 5 U.S.C. § 552(a)).

272. For notable calls for a new federal privacy policy body, see Peter Swire, *Why the Federal Government Should Have a Privacy Policy Office*, 10 J. TELECOMM. & HIGH TECH. L. 41 (2012); Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L.J. 1183 (2003).

273. Again, the CEQ provides a useful model: Between 1970 and 1997, the Council on Environmental Quality issued annual Environmental Quality Reports pursuant to NEPA § 201. In 1995, Congress passed the Federal Reports Elimination and Sunset Act, Pub. L. No. 104-66, 109 Stat. 707, that eliminated the reports.

Protection Administration ("PPA")—to oversee those filings rather than one located in the White House. Administrative norms of government in the United States allow agencies in the executive office of the President to make rules that bind executive branch agencies, but domestic regulations intended to reach outside the federal government are normally formulated in a standard agency such as a cabinet department or the EPA; even so, these agencies' regulations will be subject to OMB review before issuance.[274] Significantly, the EPA benefitted from being a free-standing entity with its own administrator, rather than being part of the Department of the Interior or the Department of Commerce, where its budget, personnel, and legislative priority decisions would have been subject to inevitable trade-offs, and where the agency head would have had one or more layers between her and the President.

How far should the regulatory reach of these agencies extend? Because public and private entities share data,[275] the most effective rule would be a federal (national) rule that reached all three types of data collectors: private-sector collectors, ordinary government agencies (including state and local agencies), and national-security/paramilitary agencies.[276] A single national solution would allow the maximum standardization as to what a PIN should contain and what the carve-outs to the PINs regime should be.

The suggestion that a new permit-like requirement should be extended to large private efforts to collect personally identifiable information will be controversial; critics will say that it will be overly expensive and will interfere with innovation. These critics are partially correct; business plans that do not qualify for safe harbors or that cannot be modified to include sufficient privacy mitigation (concepts explored in the following sub-section) will suffer some expense and delay—and, if they fail to provide adequate disclosure, even greater expense and delay if they are sued. That is, in fact, one of the goals of the proposal: to create some counter-pressure that partly internalizes the externalities, thus inducing firms to forgo the privacy-damaging programs with the lowest predicted rewards.

If the political objections are too great, PINs could be introduced with a narrower reach, although they risk being less effective as a result. Instructively, NEPA's reach grew over time. The narrowest reach would be just to projects initiated by civilian federal agencies, the bodies currently required to conduct PIA's.[277] A more ambitious expansion that was still limited to federal agencies would bring in the paramilitary and national security bodies that currently conduct widespread domestic sur-

274. There are also so-called independent agencies, Article II bodies whose (often collegiate) leadership enjoy some protection from removal. Although, like NASA, the EPA is a free-standing administrative body, it is not an independent agency.

275. *See* Froomkin, *supra* note 8, at 1468.

276. *See infra* text accompanying notes 333–44.

277. *See supra* Part III.D.1.

veillance, or extend the rule to government contractors as a condition of doing business with the federal government.

Alternately, PINs legislation would have some value even if enacted only at the state level. NEPA itself only reaches federal conduct, although that includes any state projects that require a federal permit. NEPA however, has been widely imitated, with many states enacting local "little NEPA" rules.[278] Indeed, having states pass their own PINs statutes would remove any question of federalism limits on Congress's power to regulate state projects. While federalizing management and review of PINs encourages uniformity, it also centralizes power and expense. Subsidiarity concerns might counsel for having states take the lead on some regulation. Some of that might be achieved by having states take over regulation pursuant to an agreement with the federal PPA, much like states take over air and water management duties subject to federal approval. It is, however, dubious whether a federal statute could direct states to implement PINs regulation without their consent.

Although these questions of scope are difficult and important, they are logically secondary to whether the pollution analogy is persuasive, and if so whether NEPA provides a useful model worthy of emulation. Regardless of the means by which it is authorized and administered, any proposal for new constraints on private data collection must come hedged with limits in order to preserve key constitutional values such as First Amendment newsgathering and Fifth Amendment property rights. Even though these considerations do impose some constraints, they are much less severe when applied to data-gathering than if one attempted to follow the European lead and regulate data-sharing, as that would cover pure speech. The next Section considers the necessary limits on a PINs rule, as well as the areas where any disclosure rule ought necessarily to apply. It also discusses some of the difficult grey area between the polar cases.

E. What Privacy Impact Notices Should Cover—And Exclude

A NEPA-style regulatory strategy aimed at surveillance technology will divide privacy-harming technologies and practices into three broad categories: (1) Technologies and practices that are outside the scope of regulation and that do not need to file a PIN (i.e. things that fall into one of the Categorical Exclusions);[279] (2) Technologies and practices not covered by any CE, which, while capable of causing substantial harm to privacy, can be mitigated sufficiently to escape further regulations (i.e. things qualifying for a mitigated FONSI); and (3) Technologies and practices so destructive of privacy, or for which any attempt at substantial

278. *See* Patrick Marchman, "Little NEPAs": State Equivalents to the National Environmental Policy Act in Indiana, Minnesota and Wisconsin (Sept. 2012) (unpublished capstone paper, Duke University), *available at* http://dukespace.lib.duke.edu/dspace/bitstream/handle/10161/5891/P.%20Marchman%20Little%20NEPAs_Final_w%20endnotes.pdf?sequence=1.

279. *See infra* Part III.E.1.

mitigation would so undermine the purpose or value of the data collection, that no FONSI could possibly apply—what I call 'red flags' below.

Congress, in enacting a PINs rule, could define certain activities as falling in each category, but inevitably the nuts and bolts task of deciding on particular applications would have to fall on the (judicially reviewable) agency charged with making those adjudicative decisions. It is beyond the scope of this Article to set out more than an illustrative list of what would fall into each of the three categories. However, in order to make clear that this proposal aims only at the largest and most invasive privacy-harming technologies, I have attempted to provide the most detailed examples of the Categorical Exclusions—activities that would trigger no analysis requirement at all.

1. Categorical Exclusions

If an activity falls within a Categorical Exclusion ("CE") that means that there is no need for further action and the activity can proceed unimpeded. What falls within CEs is critical because the people undertaking those activities will not need to take the time to formulate an application for a FONSI, much less a full PIN and will also know that they face no risk of litigation so long as they legitimately qualify for the CE. What follows is a non-exhaustive list of proposed Categorical Exclusions for the PINs process.

Categorical Exclusions should cover activities that have constitutional protection, notably core First Amendment activities such as newsgathering.[280] Drawing the line between newsgathering on the one hand, and collecting data in the hopes of learning something interesting and perhaps publishable on the other, is not easy. Nevertheless, there is a distinction between following an elected official to see if she is meeting with lobbyists in the evenings and recording the movements of a million people in hopes of learning which are the hottest new restaurants. Not only is there a distinction in terms of scale, but the watch on the politician's activities is a core type of protected speech.[281] Alternatively, one might say that one set of actions is public-regarding, or "governance related" while the other is "private-regarding."[282]

In addition, CEs should cover all activities initiated by a property owner (or lessee) that take place on that person's private property so long as it is a place where the public at large is not ordinarily invited, such as the home. Furthermore, data collection by third parties in these

280. A CE for all First Amendment activities makes sense only if one understands the First Amendment protection for data gathering to be less then absolute. Were one to take the most expansive view, as does Jane Bambauer in *Is Data Speech?*, 66 STAN. L. REV. 57 (2014), the exception would entirely swallow the rule.

281. Relying in a distinction between core and non-core speech carries doctrinal baggage, as it risks eliminating the content-neutrality that allows PINs to be subject to only intermediate scrutiny. *See infra* text at notes 356, 381. In such cases it may be necessary to fall back on even more neutral distinctions based on either the type of technology used or the number of people effected.

282. *See* Joel R. Reidenberg, *Privacy in Public*, 68 U. MIAMI L. REV. 141, 155 (2014).

primarily private spaces should also be covered by CEs so long as the same conditions are met and the owner or occupier explicitly approves or at least has the ability to stop the data collection without adverse consequences. CEs should also cover all small-scale activities for which the cost of complying with the PINs requirement would be grossly out of proportion to even the maximum potential harm to privacy.

More controversially, I think CEs should cover data collection preceded by meaningful consent,[283] even though this can permit an enormous amount of data-collection depending upon how broadly one defines meaningful consent.

First Amendment Activities. To begin with, it is essential that CEs extend to all activities incident to ordinary reportorial behavior.[284] Thus, filming or recording spot news, even mass demonstrations, for the purposes of newsgathering or reporting, would not trigger any reporting requirement. Similarly, a demonstrator's recording of fellow demonstrators would clearly be outside of any PINs requirement. A harder case would be presented, however, by police attempts to process recordings by an undercover informant in order to identify large numbers of the persons present at an event through, say, facial recognition. Here there is no First Amendment right at issue. Thus, at some point—perhaps in the absence of reasonable suspicion that those recorded had committed a crime—the police's collection of film or photos in order to identify faces would fall outside the clear confines of a CE and into one of the potential reporting categories.

Public Officials. Any data collection relating to a public official's or employee's performance of his or her duties in a public place would be automatically covered by a CE in order to eliminate any risk of intrusion on the core First Amendment role of the press in monitoring and checking the government. The CE would include recording the actions of police and other government employees in public places, while not covering the routine placing of recording devices in offices or other places where workers are entitled to expect some privacy. (A one-off recording, such as a sting operation, would fall under the next CE, for small-scale activities.)

Small-Scale Activities. More generally, any common, visible data collection activity that affected only a relatively small number of people annually would automatically qualify for a CE.[285] Thus, for example, small-scale personal films or recordings for personal use, such as a tourist's filming of a vacation, would automatically fall under a CE. Just as we do not require EISs every time someone proposes to smoke a cigarette, so too we should exempt small-scale personal data collection such as eve-

283. As noted above, see *supra* text at note 81, not all legal consent is meaningful.

284. A similar exclusion is found in Article 9 of the Data Protection Directive. *See* Data Protection Directive, *supra* note 145, at Art. 9.

285. I have kept the exact number vague as any specific number is arbitrary. I would imagine anything in the hundreds would clearly be outside of scope, and perhaps more.

ry time a person posts a picture on Instagram.[286] Whether a similar rule should apply to uncommon or unexpected or invisible methods of data collection that affected only a small number of persons is a more difficult question.[287]

Meaningful Consent. Any data collection resulting from truly informed consent—e.g. data collected pursuant to a medical study in which the subjects agreed to participate after having the data collection and use explained to them—should be entitled to a CE. Even if this were to exclude a great deal of medical data, the disclosure of that data is currently regulated through other channels, including HIPAA[288] and the HITECH Act.[289]

A more difficult question is whether other data-gathering contracted for with adequate individual notice and formality should be covered by a CE. The problem here begins with the reality that most standard-form consumer contracts simply do not get read or are not understood by most consumers.[290] On the other hand, our courts—perhaps mistakenly—enforce them. Denying a CE to collection pursuant to these agreements would have the advantage of reflecting an important reality that much unseen information collection about consumers happens pursuant to legally valid contracts. Conversely, giving a CE to all consumer data collection pursuant to a written agreement would create a very broad exception and would likely extend to many consumer contractual relationships in which money changed hands—including cell phone tracking by cell phone providers.[291]

One argument for creating a CE for cell phone and other written agreements is that it would allow the PINs effort to start small while we

---

286. If the proposals in this article are extended to virtual spaces, then one might apply them to a program designed to systematically apply facial recognition algorithms to Instagram or Facebook photos. *See infra* Part III.F.

287. Thus, for example, what if someone embarks on the thorough surveillance of, for example, fifty people, using mobile cameras, drones, and biometrics? Should that be covered? Perhaps not, on the theory that the number of people is relatively small and the application both unusual and labor-intensive. On the other hand, the PINs proposal outlined in this Article would apply to a fixed camera on a telephone pole capable of monitoring entrances and exits from a single-family home if that camera was part of a larger city-wide monitoring program.

288. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104–191, 110 Stat. 1936 (codified as amended in scattered sections of 18 U.S.C.; 26 U.S.C.; 29 U.S.C.; 42 U.S.C.).

289. Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, Pub. L. No. 111–5, 123 Stat. 226 (2009).

290. *See supra* text at note 81.

291. Whether this CE should cover cell-phone tracking by free apps so long as the disclosure of the tracking was sufficiently prominent to be meaningful is a harder question. The proposed Application Privacy, Protection, and Security (Apps) Act of 2013, H.R. 1913, 113th Cong. (2013), would make these disclosures mandatory. Certainly at present many users are not aware of the extent to which apps track and record their cell-phone behavior and personal movements, and app-makers are not racing to disclose these facts. *See, e.g.*, Robert McMillan, *Siri Remembers Your Secrets, But for How Long?*, WIRED (Apr. 18, 2013, 6:30 AM), http://www.wired.com/ 2013/04/siri-privacy/ ("Not everyone realizes this, but whenever you use Siri, Apple's voice-controlled digital assistant, she remembers what you tell her. How long does she remember? Apple isn't saying."); *see also* Robert McMillan, *Apple Finally Reveals How Long Siri Keeps Your Data*, WIRED (Apr. 19, 2013, 6:30 AM), http://www.wired.com/ 2013/04/siri-two-years/ ("After our story ran, Apple spokeswoman Trudy Muller called to explain Apple's policy, something privacy advocates have [been] asking for.").

get the bugs out; that is also, however, the essence of the reason not to exclude those agreements: why create a such a substantial regulatory edifice if it is going to exclude some of the most significant sources of privacy damage? Those who, quite reasonably, object that this exclusion is too great may take consolation in the tripartite thought that because these data are collected pursuant to contracts: (1) they are often subject to other types of regulation;[292] (2) if it was bargained for in a contract, it is not a classic externality; and (3) even if not freely bargained for due to being in an industry-standard form, if the surveillance is at least fully disclosed in the contract, there is less benefit to be had from a PINs disclosure.[293]

Perhaps the best compromise between covering big instances of data collection and not overwhelming the PINs system, at least initially, would be to allow CEs for contractually defined data collection so long as the disclosures in the contracts meet some threshold of completeness, accuracy, and consumer comprehensibility,[294] and so long as amount of data being collected involved falls beneath some arbitrary threshold. That threshold might be adjusted in time as we gain experience with the PINs process.

Data Collection Limited to the Collector's Private Property. The PINs proposal concerns public and virtual public spaces. It is not intended to reach private activity purely, or even primarily, in private spaces. Thus, any data collection that only covered property owned by the party doing the collection would not be covered so long as the public was not ordinarily invited onto the property and the collector provided adequate notice of the collection to other people affected.[295] CEs would thus apply to almost any data collection in the home so long as the collection was by the homeowner (or lessor). CEs would also apply to data collection in the workplace so long as workers were on reasonable notice of the collection. However, CEs would not apply to places such as retail establishments where the public was ordinarily invited, regardless of the nature of the notice (assuming that a sufficient number of persons would be affected). In short, CEs could be available even for employee biometrics collected in the workplace—so long as the employees were on proper notice—but there would be no blanket exemption for attempts to surveil

292. Cell phone providers' contract terms, however, are not heavily regulated. In particular, the Federal Communications Commission "does not regulate contractual arrangements with cellular providers." Fed. Commc'ns Comm'n, *FAQs - Wireless Phones*, FCC.GOV,, https://www.fcc.gov/encyclopedia/faqs-wireless-phones (Sept. 29, 2014).

293. Admittedly, a PINs disclosure would require some discussion of the likely uses and of synergies with other data sources, so the contractual disclosure is almost inevitably going to be less complete.

294. The Consumer Financial Protection Bureau's "Know Before You Owe" project may provide a model. *See Know Before You Owe*, CONSUMER FINANCIAL PROTECTION BUREAU, http://www.consumerfinance.gov/knowbeforeyouowe (last visited June 6, 2015).

295. Thus, for example, an ordinary home would qualify even if tradespersons sometimes came to the home, but a show home intended for prospective buyers would not be covered. The EU Privacy Directive contains a similar exclusion for households in Article 3 of the E-Privacy Directive. *See* E-Privacy Directive, *supra* note 144, at Art. 3.

customers or random passersby. In addition, this CE would not apply to third-party data collection in, or aimed at, primarily private spaces.

Conspicuous Off Switch. Anything with a conspicuous and reasonably understandable[296] off switch entirely controlled by the subject of the surveillance ought to enjoy a CE. The logic here is similar to that of the meaningful consent prong; if the off switch is conspicuous and really in the control of the data subject then the choice not to use it is a form of meaningful consent. This category could include third-party collection devices such as smart meters if the subject had the ability to turn off the collection. Without a conspicuous off switch, however, a state-wide smart meter program would require additional analysis, perhaps qualifying for a mitigated FONSI, or perhaps not, depending on the circumstances.

As an illustration of how these CE's would work, consider clothing retailer Nordstrom's policy of tracking consumers' movements via their cell phones using the Euclid Analytics monitoring system.[297] Nordstrom put up small notices advising those consumers not wishing to be tracked to turn off their cell phones.[298] But consumers would not necessarily see these, and entering the store with a cell phone on does not amount to informed consent as we know it. Nordstrom's customer monitoring is not a First Amendment activity, and is not aimed at public officials in performance of their duties. Tracking all the cell-phone carrying consumers in a single large clothing store like Nordstrom is not "small scale" in any meaningful sense of "small" and even more so if the monitoring extended to all 271 Nordstrom stores operating in thirty-six states.[299] Nor would Nordstrom qualify for the "off switch" CE, because the off switch in question is not on the tracking device, but on something belonging to the customer. It would not qualify for the private property CE because, although Nordstrom owns or leases its premises, they are ordinarily open to the public. Thus, a tracking policy of this sort would require further analysis and disclosure; suitable mitigation, such as aggregating the data then deleting the originals, or removing all personally identifiable infor-

296. Terms like "conspicuous" and "reasonably understandable" will require contextual definition by the implementing agency.

297. *See* Angela Martin, *Nordstrom Using Smart Phones to Track Customers Movements*, CBSDFW.COM (May 7, 2013, 10:05 PM), http://dfw.cbslocal.com/2013/05/07/nordstrom-using-smart-phones-to-track-customers-movements/; *see also* Quentin Hardy, *Technology Turns to Tracking People Offline*, N.Y. TIMES (Mar. 7, 2013, 2:52 PM), http://bits.blogs.nytimes.com/2013/03/07/technology-turns-to-tracking-people-offline/ (reporting that Euclid has used 50 million customers' smart phones in 4,000 locations to monitor "how many people are coming into a store, how long they stay and even which aisles they walk"); *cf.* Press Release, Sen. Charles E. Schumer, Schumer Reveals: Stores Are Tracking Shoppers Movements Through Their Cellphones With Rapidly Increasing Frequency, and Testing Ever More Invasive Technologies; Calls For FTC to Require Mandatory "Opt-Out" Opportunity Before Retailers Are Allowed to Track Shoppers' Movements (July 30, 2013), *available at* http://www.schumer.senate.gov/newsroom/press-releases/schumer-reveals-stores-are-tracking-shoppers-movements-through-their-cell-phones-with-rapidly-increasing-frequency-and-testing-ever-more-invasive-technologies-calls-for-ftc-to-require-mandatory-opt-out-opportunity-before-retailers-are-allowed-to-track-shoppers-movements.

298. *See* Martin, *supra* note 297.

299. *See Nordstrom*, WIKIPEDIA, https://en.wikipedia.org/wiki/Nordstrom (last updated Feb. 19, 2015, 8:28 AM).

mation such as MAC and International Mobile Station Equipment Identity ("IMEI") numbers[300] and replacing them with random numbers, would qualify Nordstrom for a mitigated FONSI.[301] If Nordstrom wanted to keep the raw data for internal use, or to sell it, that would require the full PIN process—a published report explaining what they were doing.

Nordstrom, incidentally, abandoned its customer tracking days after it became public,[302] demonstrating that public information about the use of monitoring technology can deter its use. On the other hand, Google recently started "beta-testing a program that uses smartphone location data to determine when consumers visit stores,"[303] something consumers may have consented to when they signed in for Google location services. The Google case is much more challenging than the Nordstrom case, because Google provides a number of free services for consumers; email, search, and mapping are major reasons why people buy Android smart phones. Google makes the use of those services contingent on standard-form consent, but because of the breadth of activities that could be subjected to monitoring, far more than I think almost any users of the service understand, that consent might not rise to the level of "meaningful consent" sufficient to trigger a CE.[304]

2. *Red Flags*

The need for PINs is perhaps most evident in large, centralized collection schemes invisible to the subject, such as a plan to put sensors on skyscrapers. But a city-wide plan to deploy smaller, more focused cameras tied together in a network could have a similar reach even if no individual sensor covered much ground or would affect an appreciable percentage of the city's inhabitants. Thus, any technology capable of persistently capturing personally identifiable information of a substantial number of persons in public should trigger a PINs analysis to see whether it includes mitigation techniques sufficient to qualify for a mitigated FONSI or whether the collector would need to work up a full PIN.

Both the Domain Awareness System[305] and CUSP's plans to collect data about New York City[306] discussed above would trigger a PINs analysis because neither would qualify for CEs. Other examples of projects

300. An IMEI is a 15-digit number that uniquely identifies a wireless phone or other device. *About IMEI numbers*, AT&T, http://www.att.com/esupport/article.jsp?sid=KB100016&cv=820#fbid=3r_qshLu0ZN (last visited Apr. 3, 2015).

301. Recall that a FONSI is a "finding of no significant impact" made by the administering agency.

302. Angela Martin, *Nordstrom No Longer Tracking Customer Phones*, CBS-DFW (May 9, 2013, 10:43 PM), http://dfw.cbslocal.com/2013/05/09/nordstrom-no-longer-tracking-customer-smart-phones/.

303. John McDermott, *Google Takes Its Tracking Into the Real World*, DIGIDAY (Nov. 6, 2013), http://digiday.com/platforms/google-tracking/.

304. *See supra* Part III.E.1.

305. *See supra* Part II.A.1.

306. *See supra* Part II.A.2.

that would undoubtedly require further analysis include Google Glass,[307] Google StreetView,[308] Google's survey of Wi-Fi signals,[309] and California's plan for statewide monitoring of private energy consumption via a "smart grid."[310]

Surveillance of Persistent Protests. Persistent protests such as Occupy Wall Street attract attention from law enforcement[311] and the media. In the course of these activities, large numbers of persons may be recorded, and identified by observation or by the use of mechanized facial recognition. Should news organizations covering these on-going events benefit from the First Amendment exception? And what about law enforcement investigative actions undertaken in advance of any reported crime? These are conversations worth having, and would be better informed by a statement delineating what sorts of surveillance law enforcement agencies contemplate.

Sporting Events. The idea that mass sporting events are targets for terrorism and other crimes long predates the 2013 attack on the Boston Marathon,[312] prompting suggestions that all attendees at events such as the Super Bowl should be scanned for automated facial recognition in the name of security.[313] This may, or may not, be popular with sport fans. Until they are told precisely what will be done with the information, there is no way fans could be expected to make a meaningful judgement.

Projects that do not fall into one of the broad categories defined by the CEs would not usually be required to produce a full report on their privacy impacts. The agency responsible would then do a preliminary study (like an Environmental Assessment[314]) to determine whether the privacy impacts are small (a FONSI) or whether, in light of mitigation strategies proposed by the party planning the monitoring, a mitigated

---

307. *See, e.g.*, Jared Newman, *The Real Privacy Implications of Google Glass*, TIME (May 2, 2013), http://techland.time.com/2013/05/02/the-real-privacy-implications-of-google-glass/; *see also* David Kravets & Roberto Baldwin, *Google Is Forbidding Users From Reselling, Loaning Glass Eyewear*, WIRED (Apr. 17, 2013, 3:00 PM), http://www.wired.com/gadgetlab/2013/04/google-glass-resales/; Claire Cain Miller, *Google, Emulating Apple, Restricts Apps for Glass*, N.Y. TIMES, Apr. 17, 2013, http://query.nytimes.com/gst/fullpage.html?res=940DE7DD133EF934A25757C0A9659D8B63 (reporting that Google will be "much more restrictive" about apps for Google Glass than for its other products in order "to deal with concerns like privacy"); *cf.* Miranda Neubauer, *A New Online Petition Asks the White House to Ban Google Glass*, TECHPRESIDENT (May 7, 2013), http://techpresident.com/news/23842/we-people-petition-calls-limitations-google-glass-surveillance.

308. *See Privacy and Security*, GOOGLE, http://www.google.com/maps/about/behind-the-scenes/streetview/privacy/#streetview (last visited Apr. 3, 2015); *see also* David Streitfeld, *Google Concedes That Drive-By Prying Violated Privacy*, N.Y. TIMES, Mar. 12, 2013, http://www.nytimes.com/2013/03/13//technology/google-pays-fine-over-street-view-privacy-breach.html?pagewanted=all.

309. Jacqui Cheng, *Google StreetView Cars Grabbed Traffic from Open WiFi Networks*, ARS TECHNICA (May 15, 2010, 5:06 PM), http://arstechnica.com/tech-policy/2010/05/google-says-wifi-data-collection-was-a-mistake/.

310. *See supra* note 25.

311. *See* Sledge, *supra* note 33.

312. *See, e.g.*, THOMAS HARRIS, BLACK SUNDAY (2000) (positing a terrorist attack on the Super Bowl).

313. *See* Declan McCullagh, *Call It Super Bowl Face Scan I*, WIRED (Feb. 2, 2001), http://www.wired.com/politics/law/news/2001/02/41571.

314. *See supra* text accompanying notes 204–06.

FONSI is appropriate. For example, the operator of a security camera system could undertake not to index images for facial recognition and to delete tapes after a set period unless a camera had recorded evidence of a crime. Or, the operator of a sensor system designed for traffic management could undertake to degrade image quality to prevent recognition of individual cars or travelers. Only if neither type of FONSI is appropriate would the data-gatherer be required to produce a full, public privacy impact statement.

Carefully calibrating the availability of FONSIs is critical to a successful PIN regime. If FONSIs have clear mitigation requirements that function as effective safe harbors then PINs will be effective without unduly harming the interests of data collectors. If, however, the FONSIs require too little mitigation then the entire regulatory scheme becomes an almost meaningless exercise. On the other hand, if clearly specified and meaningful FONSIs are not ever available, there is a danger that too many projects will be forced to produce a full-blown PIN. Too many PINs will tax the resources of the regulators and of the intermediating organizations that read them.[315] In addition, each PIN creates an opportunity for litigation alleging that the project has not fully disclosed its privacy consequences—suits that could sometimes be brought for tactical purposes of delay.[316] The Supreme Court and Congress have become suspicious of private rights of action for this and other reasons, yet some private right of action is essential to ensure that parties obliged to produce the Privacy Impact Notices have taken the obligation seriously.[317]

3. *PINs Should Sunset*

One lesson well worth learning from our experience with environmental impact statements is that things change. The EIS regime is seriously deficient in that once an EIS is approved, it is basically good forever.[318] Over time, however, our understanding of the consequences of an environmentally sensitive activity may change as measuring technology improves or as our understanding of ecosystems (or the human body) improves. Equally importantly, ecosystems are dynamic, and are also subject to synergistic threats. An activity that may not have been environmentally significant when commenced may become important due to climate change or interactions with other pollutants. The same is true of

315. *See infra* text accompanying note 406.

316. Recall, however, that all that is at stake is issuing the notice. The PINs proposal does not impose substantive or even procedural limits on the data collection so long as the collector fully discloses the privacy impacts of a data collection practice.

317. *See supra* Part III.D.3 (describing limits to private actions enforcing Privacy Act).

318. An EIS is only required to get project approval. And even then, claims made in the EIS are not rigorously tested against the reality of the project once built. *See National Environmental Policy Act (NEPA): Compliance and Enforcement,* EPA.GOV, http://www.epa.gov/compliance/nepa/ (last visited Apr. 3, 2015); *see* Sarah Langberg, *A "Full and Fair" Discussion of Environmental Impacts in NEPA EISs: The Case for Addressing the Impact of Substantive Regulatory Regimes*, 124 YALE L.J. 716 (2014).

privacy-harming technology; cameras become a bigger threat to privacy when storage becomes cheap and when facial recognition software improves.[319] Records available online have an entirely different impact from records available by appointment in a dusty basement somewhere. Rapid changes in sensor and information processing technology ensure that the relevance and accuracy of many PINs will have a limited shelf life.[320]

PINs, therefore, should sunset—if the data collection is going to extend for more than a number of years—five perhaps?—then the entity doing the collection should revisit its assessment of the privacy consequences in light of possible new synergies with other technologies and data streams, and reissue the notices. The remedy for an inadequate analysis of an ongoing project poses a more difficult problem than the case of a proposed project which may not yet have been built and certainly will not have been turned on before the PIN is approved. Now we have a going concern, one that may be enmeshed in a web of contracts and expectations. Turning it off until its operator provides a proper accounting of its privacy consequences may be more harsh than industry, Smart City proponents, or Congress could ever bear. Perhaps the operator could be allowed to choose between turning off the system until the proper analysis is finished and operating the system but paying some sort of penalties calibrated to the number of people whose data it is collecting and how long it takes to rectify the disclosure or analysis problem.

F. PINs for Virtual Surveillance?

'Virtual surveillance' takes place on electronic networks as opposed to the three-dimensional 'meatspace' we inhabit.[321] Virtual surveillance information is easily correlated with in-person surveillance; the two are highly synergistic.[322] In an instantly notorious experiment, Alessandro Acquisti demonstrated that by using three low-quality webcam camera photos he could match the faces of college students to their Facebook profiles 31.18% of the time.[323] The pattern matching took only three seconds each. Subscribers to services such as Facebook, Instagram, and Twitter post large amounts of information about themselves, and also about others. Much of this data is available for mining by all other subscribers, and sometimes everyone with an Internet connection, subject only to some variation based on the oft-changing terms of use of these

319. We may be at that point now. *See Facial-Recognition Technology Proves Its Mettle*, SCIENCE NEWS (May 24, 2013), http://www.sciencedaily.com/releases/2013/05/130524142549.htm (describing a Michigan State University study in which investigators were able to quickly identify one of the Boston Marathon bombing suspects from a law enforcement video).

320. "[S]ignificant new privacy lurches have become an increasingly common phenomenon." Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 909 (2013).

321. *'Everyone in US under virtual surveillance' - NSA whistleblower*, RT (Dec. 5, 2012), http://rt.com/usa/surveillance-spying-e-mail-citizens-178/.

322. Alessandro Acquisti, et al., *supra* note 66.

323. *Id.*

commercial services and the diligence with which the users monitor their privacy settings.[324]

This virtual surveillance becomes ubiquitous when the government uses its powers to induce firms to enable the routine collection of the content of private activities such as cell phone location data, email metadata, or the capture—whether by public or private parties—of the content of phone, internet, or voice communications. Recent revelations regarding the NSA's systematic collection of telephone calls and emails,[325] location data,[326] other internet communications,[327] including via Outlook and Skype,[328] associated metadata,[329] and mapping of personal communications networks[330] underscores how little we may know about mass surveillance aimed at all of us.

PINs offer a means to fill the void in our knowledge about virtual surveillance. As with PINs aimed at physical surveillance, the virtual surveillance disclosure requirement could be imposed on the private sector, the public sector, or both. As in physical space, no permits are currently needed to collect and re-use data that users voluntarily make available on public networks such as Twitter or Facebook, so there is no act that would trigger a PINs notice requirement. Unfortunately, the electronic and virtual realms present some obstacles that are not present in the physical case. For example, it is hard to see how one would craft a relevant permit requirement without damaging the Internet and violating the First Amendment. Also, the global nature of the Internet means that a state-based 'little NEPA' rule has no chance of effectiveness, and indeed even a national rule could be quite easily avoided from abroad.[331]

Ironically, PINs likely would be most effective if applied to the public sector—the domain where they are least likely to be adopted. The global nature of the Internet makes it difficult to impose a meaningful

---

324. In addition, a technology provider might surveil its own customers.

325. James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls*, THE GUARDIAN (Aug. 9, 2013, 12:08 PM), http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls; Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST, Dec. 4, 2013, http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

326. *See* Patrick C. Toomey, *It Sure Sounds Like the NSA Is Tracking Our Locations*, ACLU (Sept. 30, 2013, 12:36 PM), https://www.aclu.org/blog/national-security-technology-and-liberty/it-sure-sounds-nsa-tracking-your-location.

327. *See* Jonathan Stray, *FAQ: What You Need to Know About the NSA's Surveillance Programs*, PROPUBLICA (Aug. 5, 2013, 2:20 PM), http://www.propublica.org/article/nsa-data-collection-faq.

328. Glenn Greenwald et al., *Microsoft Handed the NSA Access to Encrypted Messages*, THE GUARDIAN (July, 11 2013), http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data/print.

329. *See* Administration White Paper: Bulk Collection of Telephony Metadata under Section 215 of the USA PATRIOT Act (Aug. 9, 2013), *available at* http://big.assets.huffingtonpost.com/Section215.pdf.

330. *See* James Risen & Laura Poitras, *N.S.A. 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.

331. *See* A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage*, *in* BORDERS IN CYBERSPACE 129, 142 (Brian Kahin & Charles Nesson eds., 1997).

PINs regime on, say, the harvesting of Twitter data if that data can be collected anywhere in the world,[332] although it would still be useful to know what online data U.S.-based companies were harvesting from virtual public forums and what those harvesters planned to do with it. Conversely, U.S. law enforcement and security agencies are uniquely rooted to U.S. jurisdiction, and thus are easy legal targets for PINs regulation; the problem with the imposition of a disclosure rule on public sector virtual surveillance is strictly one of political will.

If we wanted to, we could require national, state, and local governments to file public declarations of the types of mass (as opposed to targeted) surveillance they proposed to undertake domestically. Rather than depending on leakers and newspapers to tell us how much of our communications and saved data are being captured, or trusting analysts to parse public officials' statements and declassified documents with a Kremlinologist's zeal, we could simply require disclosure. Then we'd know.

Unfortunately, the idea of imposing a generalized notice obligation on the police, much less the NSA, is certain to be controversial. Critics of mass domestic surveillance will say the surveillance should be banned outright.[333] Supporters of the national security rationale will say that disclosure of even the broad contours of surveillance will undermine its efficacy.[334] These critics misunderstand the value of a notice regime. Imposing a notice obligation on the NSA before it engages in widespread domestic surveillance is not inconsistent with banning the practice. Instead, it serves as a form of insurance: If a ban turns out to be insufficiently broad to halt the practice, or if there is not a consensus on a total ban, then the PIN requirement will kick in and we will at least be able to have a debate informed by what the NSA is actually doing. Conversely, that very prospect of an informed debate is what concerns persons who fear that any disclosure of measures taken in the name of homeland security will reduce the value of those measures. To date, the NSA has been very resistant to admit that it knows, or even could know in approximate terms, how many domestic U.S. persons' communications it has captured.[335]

---

332. An international rule could be effective, but that seems even less likely than the US adopting the EU Privacy Directive.

333. *See, e.g.*, Richard Stallman, *How Much Surveillance Can Democracy Withstand?*, GNU OPERATING SYSTEM, http://www.gnu.org/philosophy/surveillance-vs-democracy.en.html (last updated Jan. 5, 2015).

334. *See, e.g.*, Lucia Graves, *Mike Rogers: Glenn Greenwald 'Doesn't Have A Clue' About NSA Surveillance*, HUFFINGTON POST (June 9, 2013), http://www.huffingtonpost.com/2013/06/09/mike-rogers-glenn-greenwald_n_3411864.html (quoting Rep. Mike Rogers (R-Mich.), chairman of the House Intelligence Committee, as saying, "Taking a very sensitive classified program that targets foreign persons on foreign lands, and putting just enough out there to be dangerous, is dangerous to us,").

335. For the ugly details see *The NSA Hides Its Domestic Collection by Refusing to Count It*, EMPTYWHEEL (Oct. 13, 2013), http://www.emptywheel.net/2013/10/13/the-nsa-refuses-to-reveal-all-the-domestic-content-it-refuses-to-count/.

Supporters of the NSA should recognize that domestic surveillance is, and is likely to remain, highly unpopular. If the agency is to have any reasonable prospect of continuing its domestic activities, it will need the sort of transparency that PINs would enforce.[336] Supporters of the NSA's activities should see this as beneficial as it will focus the national debate on what surveillance is appropriate. As Jack Goldsmith, a supporter of substantial domestic surveillance, argues, public accountability would force the NSA (which faces skepticism due do its power, scale, technology, secrecy, and intrusiveness) to address criticisms.[337] That debate would, he argues, increase public support for the NSA's activities in the long run while its absence might be fatal to what he considers important national security activities.[338]

Recommendation #35 of President Barack Obama's Review Group on Intelligence and Communications Technologies proposes that the government should develop "Privacy and Civil Liberties Impact Assessments" for big data and data-mining programs in order to "ensure that such efforts are statistically reliable, cost-effective, and proactive of privacy and civil liberties."[339] The Review Group's report distinguished these proposed "Privacy and Civil Liberties Assessments" from existing PIAs[340] by saying that the new reports would be for "broader programs that may constitute multiple systems"—a suggestion that begins to sound similar to European proposals for Surveillance Impact Assessments.[341]

There are two things to like about this recommendation, but several things to dislike. The good aspects are, first, that the proposal recognizes that information acquired via one surveillance technology should not be considered in isolation; rather different surveillance mechanisms produce linkable streams of data that come together in a complex ecosystem of information. Second, the proposal recognizes that the effects of a surveillance technology need to be considered not just when the technology is introduced, but when its effects can be seen. These good aspects of Recommendation #35 are outweighed by some bad ones. The reviews are not proposed to be routine. They are not public. And (at least explicitly) they focus on use and re-use of data, without first considering the modes of collection, although that expanded scope might be inferred from the explanatory text's mention that "policy officials should explicitly consider

336. *See* Kreimer, *supra* note 4, at 179 ("[U]ltimately in the 1970s it was the surreptitious quality of the surveillance that led to its delegitimation; programs that are openly avowed are likely to garner more long run support.").

337. Jack Goldsmith, *Reflections on NSA Oversight, and a Prediction That NSA Authorities (and Oversight, and Transparency) Will Expand*, LAWFARE (Aug. 9, 2013, 7:52 AM), http://www.lawfareblog.com/2013/08/reflections-on-nsa-oversight-and-a-prediction-that-nsa-authorities-and-oversight-and-transparency-will-expand/.

338. *Id.*

339. PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMC'NS TECHNS., LIBERTY AND SECURITY IN A CHANGING WORLD 229–30 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

340. *See supra* Part III.D.1.

341. *See* SAPIENT FINAL REPORT, *supra* note 184.

the costs and benefits of a program if it unexpectedly becomes public. In some cases, that consideration may result in modifications of the program, or perhaps even in a decision not to go forward with a program."[342] Recommendation #35 has been criticized as "vaporous" on the grounds that it "would amount in practice to additional paperwork burdens that accomplish little."[343] President Obama's speech in response to the Review Group's report made no mention of setting up the Assessments.[344]

The recent history of state-sponsored surveillance suggests that it grows rapidly in the dark; imposing a real disclosure regime, something much more public than Recommendation #35, should create some incentive for the NSA and other related agencies to stop and think before acquiring communications and data simply because it is technically feasible. So long as the disclosures are accurate, it also means that we can have a debate about privacy/security tradeoffs that is tied to an accurate picture of domestic surveillance. Democratic debate needs accurate information if it is to have any reasonable hope of coming to good conclusions.

IV. ANTICIPATING OBJECTIONS

The Constitution does not constrain our ability to put limits on government data collection even if, politically, that may be a controversial objective. In contrast, proposed limits on private data-gathering in public spaces need to be analyzed to make sure that they comply with existing First Amendment doctrine and, more generally, with First Amendment principles. In addition, any such proposal needs to demonstrate that it will not do more harm than good. We do not want a rule that will ban tourist snapshots, or one that would prevent a reporter (or any other citizen) from filming a rally, a traffic stop,[345] or even a traffic jam. Fortunately, a carefully crafted rule that reaches only systematic, repeating or continuing, sense-enhanced or machine-generated data collection that will collect potentially identifiable information about a substantial number of persons is a rule that will do none of these things.

The First Amendment issue cannot be avoided because despite the broad carve-outs proposed above, the PINs requirement will impose a licensing prerequisite—or at least a delay, which in First Amendment terms amounts to the same thing—on the largest or most intrusive data-collection projects in or through public spaces, whether real or virtual. Much of the First Amendment problem would be avoided by having a

342. PRESIDENT'S REVIEW GRP., *supra* note 339, at 230.

343. Benjamin Wittes, *Assessing the Review Group Recommendations: Part VII*, LAWFARE BLOG (Jan. 10, 2014, 3:45 PM), http://www.lawfareblog.com/2014/01/assessing-the-review-group-recommendations-part-vii/.

344. *Report Card on the President's Review Group*, ACCESSNOW.ORG, https://www.accessnow.org/pages/report-card-on-the-presidents-review-group (last visited Apr. 3, 2015).

345. *Cf.* ACLU v. Alvarez, 679 F.3d 583, 608 (7th Cir. 2012) (holding that the ACLU had a strong likelihood of success in suit for injunction against Illinois law making it illegal to "openly audio record the audible communications of law-enforcement officers . . . when the officers are engaged in their official duties in public places" because the law likely violates the First Amendment).

real-time-notice-only regime, but there is no reason at all to believe that real-time notices alone would be meaningful or effective—or even, in cases such as skyscraper-based cameras, practicable. Furthermore, if public data-gathering really is like pollution in that it imposes an externality on others, notice while the activity is going on does too little to cure the problem. We do not say, for example, to firms proposing to put large smokestacks in a residential neighborhood that their activities are fine so long as once the smoke starts flowing they send everyone downwind a letter stating that from now on they may suffer if they choose to continue to breathe.

A. First Amendment Right to Data Collection

Newsgathering is closely related to, yet distinct from the "right to receive information." This "right to receive" is "a corollary of the right to speak, meaning that audience rights stem from speaker rights."[346] In contrast, newsgathering is less passive. Rather than being about getting information someone else wants to share with you, newsgathering is about getting the information for yourself, with an implication that you may share it with others. Newsgathering is a condition precedent to reporting, which is an organized form of information-sharing. As such, newsgathering is directly protected by the First Amendment.[347] If the First Amendment applies to all citizens equally,[348] then any prohibition on public data-collection threatens to run afoul of this right.[349] And if the prohibition operates prospectively—or requires a license—then it invites the invocation of deep-seated and well-justified prohibitions on speech-related prior restraints and on speech licenses.[350]

These objections are far from fatal. Indeed, "[c]ourts usually regard information-gathering techniques as irrelevant to prior restraint analy-

346. Jamie Kennedy, Note, *The Right to Receive Information: The Current State of the Doctrine and the Best Application for the Future*, 35 SETON HALL L. REV. 789, 818 (2005).

347. *See* Red Lion Broad. Co. v. FCC, 395 U.S. 367, 390 (1969) (discussing public right of "access to social, political, esthetic, moral and other ideas"). For an especially strong assertion of the proposition that data gathering is within the core protections of the First Amendment and thus should apply with full force to most mechanized attempts to create knowledge, see Bambauer, *supra* note 280. For a vision that allows content-neutral regulation of data that does not touch core First Amendment principles, see Neil M. Richards, *Why Data Privacy Law is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501 (2015).

348. I would argue that journalists have no special rights under the First Amendment. *See* Obsidian Fin. Grp., LLC v. Cox, 740 F.3d 1284, 1291 (9th Cir. 2014); Patrick M. Garry, *Assessing the Constitutional Autonomy of Such Non-State Institutions as the Press and Academia*, 2010 UTAH L. REV. 141, 145 (2010) (arguing that journalists should not have special rights and questioning how to classify a journalist); Eugene Volokh, *Freedom for the Press as an Industry, Or For the Press As a Technology? From the Framing to Today*, 160 U. PA. L. REV. 459 (2012) (concluding that authorities suggest strongly that First Amendment protections apply to all equally). But that is not necessary for the argument in the text.

349. It also risks undermining a core First Amendment value: aiding the discovery of truth. By blocking information collection, one perforce prevents some truths from being learned.

350. *See, e.g.*, N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971) (quoting Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963)) ("'Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity.'").

sis."[351] Even if viewed through the lens of prior restraint analysis,[352] a properly limited prohibition on unlicensed data gathering in public will be viewpoint-neutral in all cases, and (depending on exactly how exceptions are formulated[353]) content-neutral in all, or almost all cases. What it may not be in all cases, however, is fast: As described below, decision-making in difficult cases may take some time. To the extent that the data-gathering is a First Amendment activity, this delay risks injuring it. The issue then becomes what level of scrutiny that injury will trigger.

A rule that applies to cameras and other sensors that collect information from or through public places is self-evidently viewpoint-neutral (in the relevant sense of ideology, although not in the sense of which way the camera faces). Similarly, the rule is content-neutral, for although it does regulate particular types of high-tech content, it does not discriminate between the content on the basis of its topic in any of the senses that the Supreme Court has forbidden.[354] As such, it will be subject to at most intermediate scrutiny. And, given the importance of the public and private values being protected, a properly drafted—neither overbroad nor vague—set of limitations on private data acquisition will pass intermediate scrutiny.[355] In general, rules that focus on the types of technology used, or on the number of people affected, or on the types of environments effected (e.g. homes), will clear the bar more easily than distinctions predicated on the more goals or purposes of the data collection, as these risk being seen as content-based.[356]

---

351. William E. Lee, *The Unusual Suspects: Journalists As Thieves*, 8 WM. & MARY BILL RTS. J. 53, 58 (1999); *see also* Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1173 (2005) (noting that "[o]rdinary public and private law rules regulating businesses engaged in the trade in customer data would be, like other forms of commercial regulation, outside the scope of the First Amendment and thus subject to rational basis review"); Shubha Ghosh, *Informing and Reforming the Marketplace of Ideas: The Public–Private Partnership for Data Production and the First Amendment* 1 (Univ. of Wis. Legal Studies Research Paper Series, Paper No. 1189), *available at* http://ssrn.com/abstract=2000102 (suggesting "[b]est practices for data commercialization that takes account of the normative framework and the First Amendment as applied to data").

352. *See* Lee, *supra* note 351, at 132.

353. *See supra* text at notes 281–83 and *infra* text at notes 356, 381.

354. *E.g.*, Ashcroft v. ACLU, 542 U.S. 656 (2004) (holding that a law that regulated only sexual speech was subject matter based and hence required strict scrutiny); Republican Party v. White, 536 U.S. 765 (2002) (applying strict scrutiny to, and striking down, a law prohibiting candidates for elected judicial office from making statements about disputed legal or political issues); United States v. Playboy Entm't Grp., 529 U.S. 803 (2000) (same); Carey v. Brown, 447 U.S. 455 (1980) (holding that a regulation that banned labor picketing was unconstitutional for subject matter discrimination).

355. *See* Lehr v. Robertson, 463 U.S. 248, 266 (1983) (stating that intermediate scrutiny means that a law will be upheld when it is substantially related to an important government purpose); Craig v. Boren, 429 U.S. 190, 197 (1976).

The argument in the text assumes that the constitutional issues are broadly similar whether a public or private body is doing the collection. For an argument that public surveillance may be more constrained than private data-gathering, see Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV. 1283 (2014).

356. *See supra* note 281. The Supreme Court's recent decision in *Reed v. Town of Gilbert, Ariz.*, 135 S.Ct. 2218 (2015) is not contrary. In *Reed* the Court struck down a sign ordinance that regulated signs based on what type of activity they mentioned because the law discriminated on the basis "of the topic discussed or the idea or message expressed." *Id.* at 2230–31. If PINs apply to all types of data collection in public then there could be no claim of content-based regulation. Similarly, a rule that discriminated on the basis of the amount of data, or the number of people captured, or even the type of

A better analogy—or a firmer doctrinal foundation—relies on existing licensing regimes, such as parade permits, that constrain speech but are allowed to do so long as they are appropriately tailored time, place, and manner restrictions.[357] To be valid such a licensing scheme must have an important purpose.[358] I will assert, without trying to prove it here, that saving some element of personal privacy against the kinds of assaults described above[359] is a sufficiently important reason for the proposed PINs rule. Anyone who does not agree has, I think, either little taste for privacy,[360] or has given in to the fatalism that the battle for privacy is basically lost.

Second, the licensing scheme must reduce the discretion of the officials administering it to minimize the chance of content-based censorship. This requirement is less applicable to a rule that interferes with data-gathering as opposed to one censoring speech because it is difficult to engage in viewpoint-based limitations on sensors. One usually does not know (although one may well suspect) what the sensors will reveal before deploying them, or else there would be little reason to pay for them. Even so, I will admit that if the rules are poorly drafted viewpoint-based or content-based discrimination would be possible, putting additional pressure on the rule-drafting agency to be as specific as possible about what is banned and what is permitted. That said, if we want to encourage trade-offs in which we permit sensor deployment when we hope the data revealed will be of the greatest social value, but also wish to discourage those deployments that destroy more privacy than they are worth, then we are inevitably juggling near-incommensurables. A flexible rule can provide standards, but there is an issue as to how many bright lines it can draw. That does create a risk of arbitrariness, but no worse than what in other contexts we rely on the judicial review of administrative decisions to prevent.

Third, any sensor-licensing regime must have careful procedural safeguards for First Amendment reasons and because it is the right thing to do—if only to avoid unduly blocking new business models and other socially valuable activities. On the other hand, the reasons that animate the strong policy in favor of very quick action when a prior restraint

---

monitoring technology used would not be viewpoint- or topic-based; although different types of technology capture different types of information, the difference is not easily classed as topic like. The only potential problem arises when the PINs regime begins to offer safe harbors (CEs) for certain types of speech, e.g., newsgathering. One might then argue that imposing a less stringent rule on newsgathering data collection is akin to imposing a less stringent sign regulation on "ideological signs," or "political signs." I am not convinced that this analogy holds, but if it did, either PINs would have to be defined very strictly in terms of technology or data quantity, or they might become subject to strict scrutiny on the ground of differential regulation of information based on content. Given the great importance of privacy, it is possible that such a PINs rule might survive even strict scrutiny, but strict scrutiny is unquestionably a high bar.

357. KATHLEEN ANN RUANE, CONG. RESEARCH SERV., 98-815, FREEDOM OF SPEECH AND PRESS: EXCEPTIONS TO THE FIRST AMENDMENT 9 (2014).

358. *See, e.g.*, Cox v. New Hampshire, 312 U.S. 569 (1941).

359. *See supra* Part II.A.

360. There clearly are some such people, as hundreds of thousands of Facebook pages attest.

threatens speech[361] are attenuated, if present at all, when the issue is long-term, systematic data-gathering activities like Google Street View, Google Glass,[362] the FBI's "Next Generation Identification"[363] or urban skyscraper cameras—so long as the rules are at least crafted to automatically allow (i.e. exclude from coverage) all traditional spot newsgathering activities such as filming a rally.

The most relevant case may be *Bartnicki v. Vopper*,[364] in which the Supreme Court said it would violate the First Amendment to impose liability on a third-party recipient of an illegally recorded phone conversation.[365] In *Bartnicki*, the radio broadcaster who published the conversation had no role in recording it, and the conversation indisputably concerned a matter of public importance.[366] The case, and especially Justice Breyer's concurrence, emphasized that the broadcaster had acted legally, unlike the person who originally made the recording.[367] I would argue that *Barnicki*—which I think was a hard case but was correctly decided—underlines the importance of preventing personal information from being collected in the first place. Once personal information is collected, it will often leak, and once it leaks there may be little if anything U.S. law can do about it.[368]

We can, however, expect an increasing number of cases in which private actors complain of limits on their ability to collect information either from customers or about the public. The *Sorrell* case was only a beginning, and one in which the issue was more whether information once collected could be shared rather than whether it could be collected at all.[369] Already companies wishing to assemble databases of license plate reader data have sued to overturn state laws in Arkansas and Utah prohibiting this collection.[370]

---

361. *See, e.g.*, Teitel Film Corp. v. Cusack, 390 U.S. 139, 141–42 (1968) (holding that a fifty- to fifty-seven-day delay was too long).

362. *Cf.* Carly Page, *Google Glass Will Be Banned in Las Vegas*, THE INQUIRER (Apr. 9, 2013, 2:31 PM), http://www.theinquirer.net/inquirer/news/2260225/google-glass-will-be-banned-in-las-vegas (describing spread of measures banning augmented reality eyewear with recording capabilities).

363. *See Next Generation Identification (NGI)*, FBI, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited Apr. 3, 2015); *see also* Sebastian Anthony, *FBI Launches $1 Billion Nationwide Facial Recognition System*, EXTREMETECH (Sept. 7, 2012, 1:08 PM), http://www.extremetech.com/extreme/135665-fbi-launches-1-billion-nationwide-facial-recognition-system. NGI will aggregate "fingerprints, DNA profiles, iris scans, palm prints, voice identification profiles, photographs, and other identifying information." In addition, "[t]he FBI will use facial recognition to match images in the database against facial images obtained from CCTV and elsewhere." *EPIC v. FBI - Next Generation Identification*, EPIC, http://epic.org/foia/fbi/ngi/ (last visited Apr. 3, 2015).

364. 532 U.S. 514 (2001).

365. *See id.* at 517–18, 535.

366. *Id.* at 525.

367. *Id.* at 525, 535 (Breyer, J., concurring).

368. See VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2011), for an argument in favor of a "right to be forgotten."

369. *See* Sorrell v. IMS Health, Inc., 131 S. Ct. 2653, 2668 (2011).

370. Cyrus Farivar, *Private Firms Sue Arkansas for Right to Collect License Plate Reader Data*, ARS TECHNICA (June 11, 2014, 6:45 AM), http://arstechnica.com/tech-policy/2014/06/private-firms-sue-arkansas-for-right-to-collect-license-plate-reader-data/. The Utah case was settled after the state

B. Environmental Impact Statements Are (Allegedly) a Poor Policy Tool

The standard-form critique of the EIS regime has three parts. The first attacks it for not actually requiring anything specific about environmental quality.[371] In theory, a perfectly described project for poisoning a neighborhood could have a procedurally valid EIS that was so thoroughly crafted that it would withstand even the toughest "hard look" judicial review. The second part derides the EIS-writing exercise as comprised of make-work, boilerplate, and Cover Your Ass. Court decisions finding that agencies had not considered all the relevant alternatives encourage project proponents to throw everything they can find into an EIS.[372] The result, critics say, is a bloated and unreadable document containing information of dubious quality.[373] (An alternate form of critique derides the judicial review of EISs as having become toothless, pointing to a series of Supreme Court decisions that made it more difficult to successfully challenge an EIS as inadequate.[374]) The third point is to dismiss the entire EIS edifice as a source of massive and largely pointless expenditure coupled with the potential of somewhat arbitrary and ultimately fruitless delay.[375]

There is truth in all these criticisms, but they are also somewhat exaggerated and off-target. To the extent that they are true, in some cases their force either does not carry over well into the privacy context, or their impact can be limited in light of lessons learned from the NEPA experience.

There is no question that NEPA imposes costs on parties seeking project approval. But this is hardly a fair criticism since, at least up to a point, *that is the very purpose of the statute.* NEPA intentionally shifts costs of collecting and organizing information on the environmental consequences of covered projects to the government (or to the permit applicant) rather than placing it on the project's less organized and usually less-well-financed opponents. The issue is whether the costs exceed the benefits, not whether costs exist.[376]

---

amended the statute. *Id.* The Arkansas Automatic License Plate Reader System Act is codified at ARK. CODE ANN. §§ 12-12-1801 to 1808 (2014).

371. *See* Robertson v. Methow Valley Citizens Council, 490 U.S. 332, 353 n.16 (1989) ("NEPA merely prohibits uninformed—rather than unwise—agency action.").

372. *See, e.g.*, 1 FRANK B. CROSS, FEDERAL ENVIRONMENTAL REGULATION OF REAL ESTATE § 1:8 (2014); Bradley C. Karkkainen, *Bottlenecks and Baselines: Tackling Information Deficits in Environmental Regulation*, 86 TEX. L. REV. 1409, 1409 (2008).

373. *Id.*

374. For an argument that, contrary to conventional wisdom, NEPA has actually faired reasonably well in the courts, see Richard Lazarus, *The National Environmental Policy Act in the U.S. Supreme Court: A Reappraisal and a Peek Behind the Curtains*, 100 GEO. L.J. 1507, 1511–12 (2012).

375. *See, e.g.*, Jim Rossi, *Participation Run Amok: The Costs of Mass Participation for Deliberative Agency Decisionmaking*, 92 NW. U. L. Rev. 173, 180 (1997) (noting critique of EIS process that it can "create information problems for decisionmakers and participants, encouraging use of strategic tactics, such as delay, that thwart the development of agency programs and the achievement of regulatory goals").

376. *See* Karkkainian, *supra* note 212, at 910–11.

There is also truth in the claim that the incentive for parties who want to have a project approved is to go overboard in EIS, leading to very large documents. On the one hand, this imposes needless costs on preparers, while also imposing unnecessary costs on anyone tried to read the thing. But on the other hand, given that our, at best, partial understanding of the nature of privacy harms, not to mention how new techniques will add to them, it may be healthy to err on the side of overegging the disclosures, at least as compared to our present practices that frequently amount to pretending they do not exist.

Similarly, there is no doubt that NEPA can impose sometimes quite long delays on major projects. It takes time to prepare an EIS, and it can take a long time to defend it if the EIS is challenged in court. On the other hand, the large majority of projects covered by NEPA never make it to the EIS stage because they are covered by a CE or make a successful case for a FONSI,[377] and a well-structured PINs regime would aim for similar outcomes. It may not be an entirely bad thing that a small number of projects with the most serious foreseeable environmental impacts are subjected to more extensive public deliberation—and, in the case of inadequate disclosures, a lawsuit—before being allowed to proceed, even if in extreme cases the delay may have been longer than is reasonable.

A regime whose primary effect was to cause firms to produce a public PIN could be an enormous gain for privacy. In addition, the compliance process of producing the PIN would create an occasion for organizational reflection. The PIN process would not only put privacy on the agenda, the PIN's publication would make privacy encroachments visible—curing information asymmetries, and perhaps creating public counter-pressure. Even the threat of this counter-pressure will put the risk of bad public relations into the decisional mix, causing proponents of less valuable potentially privacy-harming projects to modify or cancel them.[378] As noted above, the U.S. government already conducts internal Privacy Impact Assessments ("PIA");[379] albeit one without much in the way of incentives to maintain quality in the analysis and disclosure. PINs would correct the incentives and add a public component. PIAs are used in Europe; they may be less common in U.S. industry, but they are far from unheard-of.[380]

Speed is an issue, especially in the context of high-tech products involving either sensors or data processing, areas in which the technology is changing rapidly. Any PIN system that routinely took years to produce a

---

377. *See id.* at 920.

378. *See* Charles Raab & David Wright, *Surveillance: Extending the Limits of Privacy Impact Assessment*, *in* 6 PRIVACY IMPACT ASSESSMENT 363, 363 (David Wright & Paul De Hert eds., 2012).

379. *See supra* Part III.D.1.

380. *See* David Wright, *Should Privacy Impact Assessments be Mandatory?*, 54 COMM. ACM 121 (Aug. 2011), *available at* http://cacm.acm.org/magazines/2011/8/114936-should-privacy-impact-assessments-be-mandatory/fulltext; David Tancock, et al., The Emergence of Privacy Impact Assessments (May 21, 2010) (unpublished manuscript), *available at* www.hpl.hp.com/techreports/2010/HPL-2010-63.pdf.

result would risk making many data-collection projects irrelevant and uneconomic by the time they emerged from the regulatory pipeline. The speed issue arises in the environmental context also, and the Obama administration has responded with a series of regulations designed to stimulate the creation of fast-track procedures.[381] Among them are five pilot programs that the Council on Environmental Quality is currently evaluating for efficiency and effectiveness,[382] some of which are possible models for a streamlined PIN system. In any event, much will depend on the proposed PPC's ability to define CEs and recommended mitigation strategies that will allow the full PIN process to be reserved for the most significant potentially privacy-harming projects.

On the other hand, it should be relatively easy to craft obligations to monitor how much data are actually being collected, and also to check compliance with mitigation measures. The data, after all, are being collected anyway, are self-authenticating, and are the facts that the reviewing agency would want to know. This differs substantially from the environmental context, where a physical process must be monitored, meaning that the agency will require potentially expensive monitoring equipment.

C. Notice is (Allegedly) Worthless

Arguments that notice is worthless—or at any rate that its value is vastly overrated—take many forms. A *sociology-based* set of critiques suggests that most people ignore most notices most of the time;[383] the *cognitive critique* suggests that even if people look at many types of notices, they are not likely to be able to understand them.[384] A bonus version of the cognitive critique argues that as notices proliferate, people become desensitized to them and tune them out.[385] And, to round out the picture, the *political critique* suggests that even if people read notices, they are not empowered to act on them in meaningful ways. It thus may not be surprising to find that a *results-based* set of critiques point to existing notice regimes such as FCRA or the Privacy Act, and observe that the activity that the notices should have alleviated continue to flourish.[386]

---

381. *See, e.g.*, Memorandum from the President of the United States on Speeding Infrastructure Development through More Efficient and Effective Permitting and Environmental Review to the Heads of Executive Departments and Agencies (Aug. 31, 2011), http://www.whitehouse.gov/the-press-office/2011/08/31/presidential-memorandum-speeding-infrastructure-development-through-more; Press Release, Council on Envtl. Quality, Council on Environmental Quality Issues Final Guidance to Promote Efficient Environmental Reviews (Mar. 6, 2012), http://www.whitehouse.gov/administration/eop/ceq/Press_Releases/March_6_2012.

382. *See CEQ NEPA Pilot Program*, COUNCIL ON ENVTL. QUALITY, http://www.whitehouse.gov/administration/eop/ceq/initiatives/nepa/nepa-pilot-project (last visited Apr. 3, 2015).

383. *See* BEN-SHAHAR & SCHNEIDER, *supra* note 97, at 64–65. *But see* Margret Jane Radin, Less Than I Wanted To Know: Why Do Ben-Shahar and Schneider Attack Only 'Mandated' Disclosure? (May 31, 2004) (U. Mich. Law & Econ Working Paper), *available at* http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1217&context=law_econ_current.

384. *See generally* BEN-SHAHAR & SCHNEIDER, *supra* note 97, at 101.

385. *See id.* at 104–06.

386. *Id.* at 42–47.

Here too there is an *economic critique* in suggesting that notices can be worse than nothing, and that some notices actually make people worse off[387]—ignorance may not be bliss, but certain partial knowledge may be harmful.

The structure proposed in this Article will result in a relatively small number of lengthy and complex documents with information about major data-gathering activities. The number of people who read the reports will in all but the most unusual case be a tiny fraction of the number of people whose data would be captured by the project described. The main direct consumers will be intermediaries such as public interest groups and the press.

Public awareness of PINs will in most cases be generated by the media, to whatever extent the documents are considered newsworthy, and through the mediating effect of organized interest groups. Pluralist theory is perhaps not in great fashion at present, but its account of the political process not only dovetails well in theory with a notice-based information regime, but also fits the facts. There are today a number of very expert and active privacy Non-governmental Organizations ("NGOs") that are ideally situated to interpret and act upon PINs, such as the Electronic Frontier Foundation,[388] the Electronic Privacy Information Center,[389] the Center for Democracy and Technology,[390] and the ACLU's Project on Speech, Privacy, and Technology.[391] In addition, a large number of legal and other scholars are engaged in privacy-related analysis. The annual Privacy Law Scholars Conference attracts more than two hundred and fifty attendees, plus a waiting list.[392] The Surveillance Studies network hosts events in the United States and abroad.[393] We can reasonably expect PINs to nourish an ecology of NGO activity, much as EISs have done for environmental groups such as the Sierra Club and the National Resources Defense Council, and the availability of FOIA requests has done for a host of others.[394]

---

387. *Id.* at 49.

388. *See* ELECTRONIC FRONTIER FOUNDATION , https://www.eff.org/ (last visited Apr. 3, 2015). For an example of EFF's reports on the deployment of surveillance technology, see Jennifer Lynch & Dave Maass, *San Diego Gets in Your Face With New Mobile Identification System*, ELECTRONIC FRONTIER FOUND. (Nov. 7, 2013), https://www.eff.org/deeplinks/2013/11/san-diego-gets-your-face-new-mobile-identification-system; *see also* Lynch & Bibring, *supra* note 19.

389. *See* ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org (last visited Apr. 3, 2015).

390. *See* CENTER FOR DEMOCRACY AND TECHN., https://cdt.org (last visited Apr. 3, 2015).

391. *See About the ACLU's Project on Speech, Privacy, and Technology*, ACLU, https://www.aclu.org/free-speech-technology-and-liberty/about-aclus-project-speech-privacy-and-technology (last visited Apr. 3, 2015).

392. *June 2015: The 8th Annual Privacy Law Scholars Conference*, U.C. BERKELEY SCH. OF L., http://www.law.berkeley.edu/17873.htm (last visited Apr. 3, 2015).

393. *See Archive for Conferences/Seminars/Calls*, SURVEILLANCE STUD. NETWORK, http://www.surveillance-studies.net/?cat=8 (last visited Apr. 3, 2015).

394. *See* Seth F. Kreimer, *The Freedom of Information Act and the Ecology of Transparency*, 10 J. CON. L. 1011 (2008).

Publicity can be a very effective method of regulating surveillance. Nordstrom's retreat from consumer tracking is one example.[395] For a public-sector case study, consider the case of the Seattle mesh network. Using a $2.6 million grant from the US Department of Homeland Security, the Seattle Police Department ("SPD") installed a wireless mesh network in downtown Seattle with 160 access points mounted on poles.[396] The network provides the ability to deliver Wi-Fi services to city departments, but also has the capability to track the movements of every wi-fi-enabled device—including smartphones—that enters its radius.[397] The SPD installed and activated the network without public consultation, and in possible violation of a city ordinance requiring that any department installing potential surveillance equipment must submit protocols to the city council for public review and approval within thirty days of its acquisition and implementation.[398] When a local newspaper revealed the existence of the network, the SPD rapidly announced that they were deactivating it, pending creation of privacy policies after "a vigorous public debate."[399] Similarly, New York City quietly allowed a private company to install trackers on city-owned telephone booths.[400] But within hours of Buzzfeed's revelation of the trackers' existence, the Mayor's office promised to remove the trackers.[401] In contrast, when Chicago designed a city-wide suite of sensors that would among other things detect cell-phones passing by as a way of estimating traffic, it chose not to record identifiable information about each individual device.[402] When the story went public there was no outcry.[403]

These tales teach us three things. First, that the media can be an effective institution in mediating public attention on surveillance issues and that institutions will sometimes react to this scrutiny. The second lesson

395. *See supra* text accompanying notes 297–302 (describing Nordstrom retreat from tracking in face of bad publicity).

396. David Ham, *Seattle Police Have a Wireless Network That Can Track Your Every Move*, KIROTV (Nov. 7, 2013, 8:09 PM), http://www.kirotv.com/news/news/seattle-police-have-wireless-network-can-track-you/nbmHW/.

397. *See* Brendan Kiley & Matt Fikse-Verkerk, *You Are a Rogue Device*, THE STRANGER (Nov. 6, 2013), http://www.thestranger.com/seattle/you-are-a-rogue-device/Content?oid=18143845.

398. *Compare id.*, *with* SEATTLE MUN. CODE § 14.18.20 (2013).

399. Brendan Kiley & Matt Fikse-Verkerk, *The Seattle Police Department Disables Its Mesh Network (the New Apparatus Capable of Spying on You)*, THE STRANGER (Nov. 12, 2013, 7:42 PM), http://slog.thestranger.com/blogs/slog/mobile/2013/11/12/the-seattle-police-department-disables-its-mesh-network-the-new-apparatus-capable-of-spying-on-you.

400. Joseph Bernstein, et al., *Exclusive: Hundreds of Devices Hidden Inside New York City Phone Booths*, BUZZFEED NEWS (Oct. 6, 2014, 2:00 AM), http://www.buzzfeed.com/josephbernstein/exclusive-hundreds-of-devices-hidden-inside-new-york-city-ph#.kxWoxWLe5.

401. Cora Currier, *New York Quickly Nixes Cellphone Tracking Devices in Phone Booths*, THE INTERCEPT (Oct. 6, 2014), https://firstlook.org/theintercept/2014/10/06/phone-booths-get-new-life-tracking-cellphone/.

402. David Heinzmann, *New Sensors Will Scoop Up 'Big Data' on Chicago*, CHI. TRIB. (June 20, 2014), http://www.chicagotribune.com/news/local/breaking/ct-big-data-chicago-20140621,0,2219153,full.story.

403. Jason Mick, *Chicago Installs Big Data Sensors to Watch Citizens, Promises Privacy*, DAILY TECH (June 23, 2014), http://www.dailytech.com/Chicago+Installs+Big+Data+Sensors+to+Watch+Citizens+Promises+Privacy/article36098.htm.

is at least as important: in Seattle, the SPD was able to make facts on the ground, and is unlikely to be subject to any legal action even if it violated the City's ordinance. If there had been a legal duty to make a public statement before spending the money to install the equipment, and if failure to explain the plan's privacy consequences properly was actionable, the debate over what to install and how to use it would have taken place at the status quo ante of lessened surveillance—and before the police had a sunk cost of $2.6 million of equipment designed to make tracking people easy.[404] The third lesson is that even though Nordstrom's private initiative and New York City's partnership with a private company were legal they were also creepy,[405] which is likely why the public rebelled. Chicago's initiative, by contrast, was not creepy because it did not directly collect personal data.

These tales of powerful public and private institutions abandoning their surveillance efforts when subjected to adverse publicity demonstrate that critiques of a notice regime focusing on whether individuals will find, understand, and act on PINs are misplaced. If media and privacy groups are monitoring the PIN process, PINs will make privacy encroachments more visible—ameliorating information asymmetries, and perhaps creating an occasion for public counter-pressure. If nothing else, they will require large-scale data collectors to consider the risk of bad public relations early in the decision process. Even if we rely on NGOs specializing in privacy issues to do the analysis and publicity there may be a question as to whether the public will hear, understand, or care about the issues, but the risk of comprehension failure will be reduced when advocates are writing press releases as opposed to expecting citizens to try to parse dry technical reports themselves.[406]

The supposed cancellation of the Department of Homeland Security's national license plate reader database provides a more complicated and nuanced story, but it too generally supports the proposition that when mediated through the efforts of expert NGOs the government will take account of the public's response to what people consider unjustified surveillance. On February 18, 2014, the *Washington Post* published a front-page story describing what it called a plan by the Department of Homeland Security ("DHS") to establish a national license plate tracking system, one ostensibly designed to "help catch fugitive aliens."[407] The article described a "national license plate recognition database service"

404. *See* SEATTLE MUN. CODE § 14.18.20 (2013); Hamm, *supra* note 396.

405. On the importance of the "creepy" factor in surveillance, see Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 60, 76–82 (2013).

406. Indeed, even the harshest critics of notice regimes conclude that the best disclosure regimes send the information directly to specialist intermediaries who then advise the public based on the data and their expertise. *See* BEN-SHAHAR & SCHNEIDER, *supra* note 97, at 187–88.

407. Ellen Nakashima & Josh Hicks, *Homeland Security is Seeking a National License Plate Tracking System*, WASH. POST (Feb. 18, 2014), http://www.washingtonpost.com/world/national-security/homeland-security-is-seeking-a-national-license-plate-tracking-system/2014/02/18/56474ae8-9816-11e3-9616-d367fa6ea99b_story.html.

that would tie into a database that was projected to grow to up to one billion records of vehicles locations based on observations of their license plates.[408] This database would be available not only to Immigration and Customs Enforcement for catching "fugitive aliens" but to other law enforcement agencies for other purposes as well.[409] The day after the *Washington Post* story, a civil liberties NGO, the Electronic Frontier Foundation, published a harshly critical analysis of the plan.[410] By the end of that day, the Secretary of the DHS announced that he had ordered the cancellation of the solicitation for the program.[411]

In fact, however, what the DHS Secretary canceled was neither the large-scale reading of license plates nor the creation of the database. As the ACLU revealed two days later, those programs were already *faits accomplis*; all that was being canceled was the solicitation the *Washington Post* had discovered, a plan for a better means for law enforcement agencies to access the database.[412] Although the initial response from the NGO community may have been flawed, it corrected the error quickly. And the DHS's panicked reaction to the publicity in the *Washington Post* suggests that if DHS had been forced to disclose its original plan to create the national license plate tracking system—via a Privacy Impact Notice perhaps—the database might never have been built.

PINs have another benefit aside from information-sharing: Just as the threat of having to file EISs can cause can firms to conduct internal pollution assessments in order to see if they can pollute less and avoid an EIS, so too does the threat of having to produce a public PIN create greater incentives for internal privacy impact analyses. These would cause government agencies and firms fearing bad publicity, or whatever delay and expense attended the full PINs process, to conduct rigorous internal PIAs. The compliance process of producing the PIAs (or, as the case may be, the PINs) would create an occasion for reflection. In some cases, would-be data collectors would find they could choose less intrusive means of achieving their goals—gains for privacy that are not subject to any of the critiques described above.

The most persuasive critique of the PINs idea is political—whether, even if armed with the information that a potentially privacy-harming project is contemplated, the public is capable of stopping the project. That is a genuine issue, but it is also an issue that arises in relation to every potential political conflict. PINs could provide a way to overcome

408. *Id.*

409. *See id.*

410. *See* Jennifer Lynch, *Update: National License Plate Recognition Database: What It Is and Why It's a Bad Idea*, ELECTRONIC FRONTIER FOUND. (Feb. 19, 2014), https://www.eff.org/deeplinks/2014/02/national-license-plate-recognition-database-what-it-and-why-its-bad-idea.

411. Ellen Nakashima & Josh Hicks, *Department of Homeland Security Cancels National License-Plate Tracking Plan*, WASH. POST (Feb 19, 2014), http://www.washingtonpost.com/world/national-security/dhs-cancels-national-license-plate-tracking-plan/2014/02/19/a4c3ef2e-99b4-11e3-b931-02041 22c514b_story.html.

412. *See* sosadmin, *Setting the Record Straight on DHS and License Plate Tracking*, PRIVACYSOS (Feb. 21, 2014, 5:21 PM), http://privacysos.org/node/1332.

structural and informational barriers that, by obscuring the potentially privacy-harming effects of certain technologies, make it much less likely for the political process to be invoked at all. If PINs work to raise the salience of the privacy-harming technologies enough to counteract privacy myopia and ignorance, we may reach a point where many data subjects become interested in engaging the political process. At that point, PINs would have served their purpose. Then it is up to the democratic process to function; if, on the other hand, the clamor for action is small, so be it.[413]

V. CONCLUSION

Surveillance by public and private bodies—and even by other people—is usefully modeled as a form of pollution suffered by the target of the surveillance. There are substantial economic similarities between data-gathering in public on the one hand and air or water pollution on the other. Our limited ability to monetize the costs of surveillance recalls the early days of the environmental movement when we had relatively little data about the sources of pollution and at best imprecise measurements of the specific damage to health and enjoyment of the outdoors.

The commonalities between privacy-harming technologies and pollution suggest that we can find the first step towards our solution to the mass surveillance problem in the first step towards our solution to the environmental problem. An 'action-forcing' and disclosure-based regime modeled on NEPA is justified, constitutional, and would be an improvement over the status quo. Mandated Privacy Impact Notices—Privacy Impact Analyses with teeth—as a prerequisite to the deployment of large-scale public surveillance efforts is a reasonable and measured response to an important and growing threat to personal information privacy. Requiring the proponents of many data collection projects to consider the privacy consequences of their plans will improve privacy practices generally. Requiring a much smaller group of particularly large-scale potentially privacy-harming data collection projects to document and justify those activities more thoroughly via PINs based on modernized Environmental Impact Statements will not only tend to improve in-house privacy practices, but it will also inform public debate about the trade-offs between privacy and other values.[414]

Recent experience suggests that the fear of adverse publicity can cause public bodies and corporations to reduce or eliminate the amount of personally identifiable information they choose to collect. The challenge is to learn about surveillance when so much of it is invisible. Equally important, the practice of preparing and debating public notices and

413. And if the clamor for action is large, but there is no action, that goes to larger issues of democracy.

414. Not everyone believes that surveillance is harmful. *See, e.g.*, Bennett Capers, *Crime, Surveillance, and Communities*, 40 FORDHAM URB. L.J. 959, 960 (2012) (arguing that "surveillance . . . deters crime and aids in the apprehension of criminals; it can also function to monitor the police, reduce racial profiling, curb police brutality, and ultimately increase perceptions of legitimacy").

mitigation strategies will educate experts and the public about potential harms from surveillance and about ways in which data collection can be ameliorated or limited.

A disclosure/notice regime should also have economic and competitive effects. If, as argued above, consumers suffer from systemic myopia causing them to undervalue data they are asked to disclose because they do not understand how the data are aggregated, the injection of additional information at a low cost to the individual about how much data is being collected and how data is being held and used will at least partially correct consumers' currently myopic economic vision. Consumers should then become more sensitive to the actual cost of losing privacy; this in turn should make firms more willing to compete on privacy.

PINs—public notices of plans to collect large quantities of data—will not preclude the more valuable benefits of data-collection. The notices will, however, describe the costs and benefits of proposed surveillance. This will not only enrich public debate but will help identify the aspects of data collection that may need regulation. Periodically revisiting the consequences of existing data-collection activities will further allow data collectors and the public to see if mitigation efforts are working or if unexpected uses of the data have made the collection more significant, and thus more destructive to privacy, than originally expected. The expense of preparing PINs—imposed only on the most privacy-destroying projects or those that fail to employ adequate mitigation strategies—is justifiable as a rough-and-ready means of internalizing the externality (or externality-like) costs that surveillance in and through public places imposes on the privacy that the public formerly enjoyed.

Like with the ice caps, the alternative to attempting to measure how much privacy we are destroying before it is all gone—in hopes of spurring mitigation—is not valuing privacy until it is too late do anything other than regret its loss. A better informed public could choose to vote with its dollars, its feet, or even its votes—or it could choose to do none of these. Whatever the outcome, we will at least be a few steps closer to making informed and sensible choices.

We need to act now—before we discover, after the fact, that we were privacy polar bears who sank into an information ocean.