11-2012

Personal Environmental Information: The Promise and Perils of the Emerging Capacity to Identify Individual Environmental Harms

Katrina Fischer Kuh
Maurice A. Deane School of Law at Hofstra University

Personal Environmental Information: The Promise and Perils of the Emerging Capacity to Identify Individual Environmental Harms

Katrina Fischer Kuh[*]

* Associate Professor of Law, Maurice A. Deane School of Law, Hofstra University. I presented this Article at the conference *Supply and Demand: Barriers to a New Energy Future*, cosponsored by the Climate Change Research Network and the Environmental Law Program at Vanderbilt University Law School. I also presented the Article as part of the Hofstra Junior Faculty Forum, at a Hofstra Faculty Workshop, and as part of the Faculty Colloquia at Indiana University Robert H. McKinney School of Law. I would like to thank those who took the time to attend these presentations and to read early drafts, including Albert Lin and Ezra Rosser. The Article has benefited greatly from the many thoughtful comments I received. Finally, I am indebted to Jonathan Nasca and Frank Piccininni for their research assistance.

I. INTRODUCTION

A variety of modern technologies reveal individual behaviors that have environmental consequences with increasing clarity.[1] Smart meters and related technologies detect detailed information about when and how individuals use electricity within the home.[2] Radio frequency identification ("RFID") chips embedded in recycling collection bins track household recycling behaviors, including everything from whether the household is recycling to whether its members properly separate their recyclables.[3] Regulators use aerial imagery and geographic information systems ("GIS") technology to detect violations of local building codes[4] and the illegal filling of

1. I refer to this data interchangeably as personal or individual environmental information. A variety of technologies can be used to monitor environmental behaviors. *E.g.*, TEXAS INSTRUMENTS, LEARN MORE ABOUT RFID TECHNOLOGY AND WASTE MANAGEMENT SYSTEMS, *available at* http://www.ti.com/rfid/docs/manuals/brochures/TIWasteManagement Brochure081108.pdf (describing chips that can be installed in trash receptacles and used to monitor household waste activities, including recycling); RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE 194 (2008) (summarizing Clive Thompson's review of Southern California Edison's creative efforts to encourage energy conservation, including the "Ambient Orb, a little ball that glows red when a customer is using lots of energy but green when energy use is modest"); Frederick R. Fucci & Annette Nichols, *Alternative Energy Options for Buildings: Distributed Generation*, *in* THE LAW OF GREEN BUILDINGS: REGULATORY AND LEGAL ISSUES IN DESIGN, CONSTRUCTION, OPERATIONS AND FINANCING 125, 125–68 (J. Cullen Howe & Michael B. Gerrard eds., 2010) (describing how smart metering devices can allow utilities and consumers to track power use by individual appliances); Saqib Rahim, *They Don't Talk Trash, They Track It*, N.Y. TIMES, Mar. 26, 2010, http://www.nytimes.com/cwire/2010/03/26/26climatewire-they-dont-talk-trash-they-track-it-76922.html (describing MIT programs that allow for the tracking of individual items of household trash and a device that monitors data about individual bicycle use). *See generally* Steven Lohr, *The Internet Gets Physical*, N.Y. TIMES, Dec. 18, 2011, at SR1 (describing an incipient boom in the use of low-cost sensors, including a new digital thermostat that "senses not just air temperature, but the movements of people in a house, their comings and goings, and adjusts room temperatures accordingly to save energy").

2. For a general overview of smart meter technology, or advanced metering infrastructure ("AMI"), see EDISON ELEC. INST., WHITE PAPER: SMART METERS AND SMART METER SYSTEMS: A METERING INDUSTRY PERSPECTIVE 7–12 (2011). *See also* Cheryl Dancey Balough, *Privacy Implications of Smart Meters*, 86 CHI.-KENT L. REV. 161, 165–68 (2011) (describing how smart meters can track household behaviors that consume energy).

3. Mary Catherine O'Connor, *RFID: Recycling Research by Radio*, WASTE AGE, Oct. 28, 2011, http://waste360.com/radio-frequency-identification-rfid/rfid-recycling-research-radio (describing the use of RFID tags in Charleston County, South Carolina).

4. Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321, 2356–57 (2007) ("The Baltimore city housing department has begun to use aerial photographs to locate illegal rooftop decks. The agency purchased aerial photographs of the entire city, and used software to match those images against databases of building permits.").

wetlands.[5] Interactive "ecomaps" allow city residents to compare environmental performance by zip code.[6] Even information generated for entirely distinct purposes (for example, Global Positioning System ("GPS") devices for vehicles) yields insights into environmental behaviors (for example, driving behavior related to gas consumption).[7]

At the same time that the technological capability to identify individual behaviors with environmental consequences (or environmentally significant individual behaviors[8]) is growing dramatically, many are also calling for environmental law and policy to reduce the environmental harms that those behaviors cause or exacerbate.[9] Indeed, the ability to detect and better understand the

---

5. Massachusetts, for example, established an Office of Geographic and Environmental Information (MassGIS), MASS. GEN. LAWS ANN. ch. 7, § 4A (West 2011), maintains state GIS data on a publicly available website, *available at* http://www.mass.gov/mgis/massgis.htm (last visited June 20, 2012), and uses GIS data in support of environmental regulation—the Massachusetts Department of Environmental Protection uses GIS to identify violations of the Wetlands Protection Act, APPLIED GEOGRAPHICS, INC., A STRATEGIC PLAN FOR MASSACHUSETTS' SPATIAL DATA INFRASTRUCTURE 4, 14 (2007) ("DEP developed an automated process combining aerial imagery and GIS mapping to look for changes within wetland areas over time. In a matter of months, this effort identified hundreds of potential violations and led to enforcement actions totaling hundreds of thousands of dollars . . . .").

6. *Explore San Francisco's Greenhouse Gas Emissions by Zip Code*, URBAN ECOMAP SAN FRANCISCO, http://sf.urbanecomap.org/?locale=en_US#/explore (last visited June 25, 2012).

7. NEXTRAQ, WHITE PAPER: FIVE WAYS TO REDUCE FUEL CONSUMPTION USING GPS TRACKING, *available at* http://www.nextraq.com/images/documents/wp_five_ways_to_reduce_fuel_consumption_white_paper.pdf (describing how business owners can use GPS to reduce fleet gas consumption, including by reporting on vehicle idling rates and vehicle speeds).

8. This term encompasses behaviors of individuals that, taken alone, have a negligible impact on the environment but, in the aggregate, can significantly harm the environment. Michael P. Vandenbergh, *From Smokestack to SUV: The Individual as Regulated Entity in the New Era of Environmental Law*, 57 VAND. L. REV. 515, 518 (2004) ("We are polluters. Each of us. We pollute when we drive our cars, fertilize and mow our yards, pour household chemicals on the ground or down the drain, and engage in myriad other common activities. Although each activity contributes minute amounts of pollutants, when aggregated across millions of individuals, the total amounts are stunning.").

9. *See, e.g.*, JASON J. CZARNEZKI, EVERYDAY ENVIRONMENTALISM: LAW NATURE & INDIVIDUAL BEHAVIOR (2011) (detailing the environmental impacts of everyday behaviors, reviewing existing attempts to change those behaviors, and suggesting forward-going policy approaches); Hope M. Babcock, *Assuming Personal Responsibility for Improving the Environment: Moving Toward a New Environmental Norm*, 33 HARV. ENVTL. L. REV. 117, 120–21 (2009) (discussing individual contributions to environmental problems through polluting behavior); John C. Dernbach, *Harnessing Individual Behavior to Address Climate Change: Options for Congress*, 26 VA. ENVTL. L.J. 107, 121 (2008) (advising how climate legislation can better engage individuals); Andrew Green, *Self Control, Individual Choice, and Climate Change*, 26 VA. ENVTL. L.J. 77, 81–82 (2008) (assuming that individuals "have values or norms that favor environmental action," but questioning the capacity to make choices consistent with such values and norms); Katrina Fischer Kuh, *When Government Intrudes: Regulating Individual Behaviors that Harm the Environment*, 61 DUKE L.J. 1111 (2012) (examining the feasibility of direct regulation of environmentally significant individual behaviors); Albert C. Lin, *Evangelizing*

contributions of individuals to environmental harms may itself spur action to address those harms—"[a]s with other cases where a 'do nothing' response has been presumed to be appropriate, the logic for ignoring small harms collapses as the cost of tracking and internalizing them drops."[10] Scholars suggest that a variety of strategies, some relatively novel in the context of environmental law, will likely be needed to effectively regulate environmentally significant individual behaviors.[11] These strategies for influencing individual behaviors can be grouped by type.[12] Government can

---

Climate Change, 17 N.Y.U. ENVTL. L.J. 1135 (2009) (emphasizing the role of values and evaluating strategies for changing behaviors within the American evangelical community); James Salzman, *Sustainable Consumption and the Law*, 27 ENVTL. L. 1243, 1250, 1255–56 (1997) (explaining the connection between consumption and environmental harm); Stephanie M. Stern, *Smart-Grid: Technology and the Psychology of Environmental Behavior Change*, 86 CHI.-KENT L. REV. 139 (2011) (critiquing efforts to achieve voluntary changes in individual environmental behaviors and recommending increased reliance on automated, technological approaches for reducing individual environmental harms); Vandenbergh, *supra* note 8; Michael P. Vandenbergh et al., *Implementing the Behavioral Wedge: Designing and Adopting Effective Carbon Emissions Reduction Programs*, 40 ENVTL. L. REP. 10547, 10551 (2010) (making recommendations to policymakers about how best to achieve reductions in harms from environmentally significant individual behaviors); Michael P. Vandenbergh, Jack Barkenbus & Jonathan Gilligan, *Individual Carbon Emissions: The Low-Hanging Fruit*, 55 UCLA L. REV. 1701 (2008) (identifying individual greenhouse-gas-emitting behaviors most susceptible to change and suggesting strategies for changing them); Michael P. Vandenbergh & Anne C. Steinemann, *The Carbon-Neutral Individual*, 82 N.Y.U. L. REV. 1673, 1724 (2007) (suggesting that a mixture of information provision, incentive schemes, and regulatory provisions may be needed to induce individuals to reduce their carbon footprints); Jed S. Ela, Comment, *Law and Norms in Collective Action: Maximizing Social Influence to Minimize Carbon Emissions*, 27 UCLA J. ENVTL. L. & POL'Y 93 (2009) (arguing for a national norm campaign to reduce individual GHG emissions that targets highly visible behaviors); Nathan Ostrander, Note, *Consumer Liability for Harms Linked to Purchases*, 2 ARIZ. J. ENVTL. L. & POL'Y 111 (2011) (proposing a consumption tort to hold individuals accountable for environmental harms). *See generally* THALER & SUNSTEIN, *supra* note 1, at 183–96 (observing that "[i]n the United States, national emissions limitations imposed on major pollution sources have been the rule, not the exception," criticizing this command-and-control regime, and suggesting strategies for achieving voluntary changes in individual behavior, for example by providing feedback and information).

10. Daniel C. Esty, *Environmental Protection in the Information Age*, 79 N.Y.U. L. REV. 115, 184–85, 196–97 (2004) (arguing that technological advances will render individual harms more visible and more susceptible to control: "As transaction costs fall, the efficiency gains from internalizing the externality will outweigh the administrative burden in more and more circumstances.").

11. Dernbach, *supra* note 9, at 123–24, 132, 144; Vandenbergh & Steinemann, *supra* note 9, at 1724 (explaining the need to use norm activation and traditional regulatory measures, "includ[ing] taxes or subsidies, cap-and-trade schemes, standards that regulate the efficiency of consumer projects made by industrial firms, and support for new technologies and infrastructure").

12. Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661, 662–63 (1998) (describing four constraints or modalities of regulation—law, norms, the market, and architecture—that "constitute a sum of forces that guide an individual to behave, or act, in a given way").

indirectly regulate environmentally significant individual behaviors by directly regulating the market (for example, subsidizing the purchase of hybrid cars or taxing the purchase of SUVs), architecture (for example, adopting smart growth zoning laws), or norms (for example, funding a public information campaign).[13] Government can also directly regulate environmentally significant individual behaviors by imposing mandates on individuals (for example, passing anti-idling laws that impose civil fines for excessive idling).[14]

Every modality for regulating environmentally significant individual behaviors could benefit from the kind of information about those behaviors that technology is increasingly making available.[15] For example, smart meters can provide households with more fine-grained information about electricity use, thereby supporting voluntary reductions in electricity use.[16] The explosion of access to individual environmental data thus presents a great opportunity for environmental law and policy.[17] Just as the need to use law to influence environmentally significant behaviors is becoming urgent and strategies for doing so are coming into focus, a range of technologies is poised to assist in that endeavor by generating information about individual environmental behaviors.

The use of technology to reveal individual environmental information can, however, impose privacy harms as well as yield

---

13. *Id.*; *see also* Kuh, *supra* note 9 (applying Lessig's taxonomy of regulation in the context of the regulation of environmentally significant individual behaviors).

14. Vandenbergh, Barkenbus & Gilligan, *supra* note 9, at 1723–30 (calculating the environmental benefits of changes in idling behavior and describing the use of anti-idling laws in conjunction with public information campaigns to reduce vehicle idling).

15. In calling for increased attention to the potential for automated technology to reduce individual environmental harms, Professor Stern observed the following:

> The focus on individual behavior change, and the comparative neglect of automated technology, has left gaps in both residential pollution policy and environmental scholarship. The future of environmental psychology and law will inevitably intertwine more tightly with technology to focus on how behavioral research informs technological innovation, consumer preferences, and technology adoption.

Stern, *supra* note 9, at 160.

16. *E.g.*, Elias L. Quinn & Adam L. Reed, *Envisioning the Smart Grid: Network Architecture, Information Control, and the Public Policy Balancing Act*, 81 U. COLO. L. REV. 833, 870 (2010) ("The provision of information and other signals to modify social norms and prompt pro-environmental behaviors related to energy use and demand-side appliance and energy efficiency investment are seen as effective means of drawing down demand.").

17. Indeed, technological advance, and, in particular, the opportunities that it provides to fill information gaps, present significant opportunities to improve environmental regulation. *See* Esty, *supra* note 10 (explaining how technology can reduce information gaps and thereby improve environmental regulation).

regulatory benefits.[18] And as technology eases constraints on the information that is feasible to collect, raising possibilities for using that information to support the regulation of environmentally significant individual behaviors, privacy concerns will—and should—emerge and lead to new constraints on the collection and use of that information.[19] Ultimately, the availability for regulatory purposes of the personal environmental information rendered newly accessible by technology will be defined in part by whether and how privacy concerns result in limits on the collection or use of that information. Accordingly, an appraisal of the potential regulatory benefits of technology-enabled personal environmental information must include not only a discussion of what information is technologically feasible to collect and how that information could aid regulation, but also a recognition that the ability to collect and use such information will likely be tempered by privacy-based limits.

The tension between technology and privacy is neither new nor limited to the collection of personal environmental information.[20] It has long been recognized that advances in technology—from the camera[21] to the computer[22] to RFID[23]—can expand the quality,

---

18. For discussions of the potential privacy concerns raised by smart meters, see ELIAS LEAKE QUINN, SMART METERING & PRIVACY: EXISTING LAW AND COMPETING POLICIES, A REPORT FOR THE COLORADO PUBLIC UTILITIES COMMISSION 9–16 (2009); Balough, *supra* note 2; Jack I. Lerner & Deirdre K. Mulligan, *Taking the "Long View" on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3 (2008); Sonia K. McNeil, *Privacy and the Modern Grid*, 25 HARV. J.L. & TECH. 199 (2011).

19. Privacy policies are presently developing for smart meter technology. *See infra* notes 230–33 and accompanying text.

20. Many scholars have described the privacy harms occasioned by technological advance and explored the associated legal implications, in particular with respect to government access to information. *E.g.*, CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1193 (2002) [hereinafter Solove, *Access and Aggregation*] (describing the privacy concerns associated with the maintenance of personally identifiable information in public records); Christopher Slobogin, *Transactional Surveillance by the Government*, 75 MISS. L.J. 139 (2005); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002) [hereinafter Solove, *Digital Dossiers*] (describing the privacy concerns created by the accumulation of personally identifiable information by third parties); Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's*, 66 COLUM. L. REV. 1003 (1966).

21. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 211 (1890) (discussing the privacy implications of the advance in camera technology, allowing photographers to take pictures more quickly and without the consent of the subject).

22. U.S. PRIVACY PROT. STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY APP. 5, at 61–65 (1977) (reporting to Congress and the President on "Technology and Privacy," in particular the effect of computer-based record-keeping systems on privacy).

quantity, and accessibility of personal information[24] and, in so doing, diminish privacy.[25] Technology continues to increase the ability to detect and record individual behaviors; modern computing further allows for the volumes of amassed data to be readily compiled and searched.[26] An individual's electronic trail includes everything from location information transmitted by cell phones and GPS devices in cars to information about personal consumption choices recorded during online transactions or when using store savings cards. One scholar describes "the rise of . . . 'digital dossiers' ":

> Every day, rivulets of information stream into electric brains to be sifted, sorted, rearranged, and combined in hundreds of different ways. Digital technology enables the preservation of the minutia of our everyday comings and goings, of our likes and dislikes, of who we are and what we own. It is ever more possible to create an electronic collage that covers much of a person's life—a life captured in records, a digital person composed in the collective computer networks of the world.[27]

Justice Alito offers this description:

> In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience. Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car's location at any time .... Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users.[28]

Many advocate limiting the collection, distribution, and/or use of the personal information revealed or rendered available through

---

23. *E.g.*, Serena G. Stein, Note, *Where Will Consumers Find Privacy Protection from RFIDs?: A Case for Federal Legislation*, 2007 DUKE L. & TECH. REV. 1, 20–22 (proposing federal regulation of RFID to protect privacy).

24. The term "personal information" is used throughout this Article to refer broadly to information about a specific individual. For a more in-depth discussion of the definition of "personal information," see Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1617–18 (1999).

25. Scientific advances in other fields can have similar effects. *See* Janet L. Dolgin, *Personhood, Discrimination, and the New Genetics*, 66 BROOK. L. REV. 755, 780–86 (2000) (describing the privacy concerns raised by and the inadequacy of privacy protections governing genome mapping). Additionally, technology can have other unintended effects (of which privacy incursions are simply one). For an overview of managing the unexpected or unintended effects of emerging technologies, see Albert C. Lin, *Technology Assessment 2.0: Revamping Our Approach to Emerging Technologies*, 76 BROOK. L. REV. 1309 (2011) (advocating for more robust technology assessment).

26. SOLOVE, *supra* note 20, at 2, 13–26 (describing the compilation and growth of searchable databases and observing that "[d]ata is digitized into binary numerical form, which enables computers to store and manipulate it with unprecedented efficiency").

27. *Id.* at 1.

28. United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring).

technological advance:[29] scholars warn of technology-enabled threats to privacy and freedom and propose limits on the collection and use of personal information;[30] legislatures act to limit the collection and use of such information;[31] and courts impose their own limits in some contexts.[32] Although many lament that privacy protections have not been augmented in a more comprehensive and robust way in response to new technological capabilities,[33] privacy concerns have motivated the imposition of privacy limits on a number of technologies.[34]

The literature and debate about the optimal balance between technological benefits and privacy generally,[35] as well as the law that

29. *E.g.*, Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 242 (1992) (critiquing then-existing privacy protections and proposing the establishment of a "privacy board" to police commercial information processing activities).

30. *E.g.*, Jack S. Balkin, Essay, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 15–17, 21 (2008) (identifying "three major dangers for our freedoms" posed by government use of new information-gathering and computing technology, and advocating the enactment of "superstatutes to regulate the collection, collation, purchase, and analysis of data"); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000) (arguing for restrictions on data mining to protect informational privacy); Schwartz, *supra* note 24, at 1670–81 (advocating for the application of four fair information standards to cyberspace, including through the establishment of a United States Data Protection Commission).

31. *See infra* notes 207–19 and accompanying text (describing statutory limits on the collection and/or use of personal information using RFID and smart meters).

32. *See Jones*, 132 S. Ct. at 945 (applying Fourth Amendment protections to police use of global positioning devices); *see also* Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 642 (2011) (reviewing appellate cases extending Fourth Amendment protection to digital communications despite intermediary storage).

33. *E.g.*, James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 58–81 (2003) (critiquing U.S. privacy policy in part for relying too heavily on individual self-policing and market strategies and suggesting that informational privacy be conceptualized as a societal good to support a more comprehensive regulatory approach).

34. *E.g.*, Privacy Act of 1974, 5 U.S.C. § 552a(o)–(r) (2006) (limiting the use of computerized "matching" by federal agencies); Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2511–20, 2701–07 (2006) (imposing limits on the government's unauthorized collection of information from modern forms of communication); Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2006) (imposing privacy rules on cable service providers, including limits on the collection and disclosure of personal information). Motivated in part by privacy concerns, some communities have enacted moratoriums (often disregarded by installing utilities) on the deployment of smart meter technology. *E.g.*, *Clearlake Bans PG&E Smart Meters, Utility Unfazed*, SMARTGRID TODAY (Apr. 2, 2011), http://www.smartgridtoday.com/public/Clearlake_bans_PG.cfm (describing an ordinance enacted by the city of Clearlake, California, seeking to impose a moratorium on PG&E smart meter installation).

35. *See, e.g.*, Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 483–84 (describing the need to balance privacy against countervailing interests); Westin, *supra* note 20, at 1206 (discussing the need for "a structured and rational weighing process with definite criteria by which public and private authorities can gauge claims for disclosure or surveillance

has developed in some contexts to define that balance,[36] can greatly inform thinking about how the balance between regulatory benefits and privacy will or should be struck in the specific context of personal environmental information. However, important context-specific considerations will ultimately shape this inquiry.[37] For an optimal balance to be struck in the context of personal environmental information—a balance that embodies a deliberate and thoughtful weighing of regulatory benefits and privacy values[38]—policymakers will need to understand the potential environmental benefits offered by access to personal environmental information as well as the associated privacy costs.[39] Both of these variables are, to a significant degree, context specific. Identifying the benefits of access to personal environmental information requires an understanding of how that information could enhance the regulation of environmentally significant behaviors. Similarly, the privacy costs of obtaining personal environmental information will be defined by considerations specific to the collection and use of the information in support of regulation and, possibly, an evaluation of the value of privacy in

---

through new devices" to balance privacy with other competing values and proposing balancing criteria).

36. Stephen Breyer, *Our Democratic Constitution*, 77 N.Y.U. L. REV. 245, 263 (2002) (describing the tension between technology and privacy and encouraging active debate to achieve a thoughtful resolution).

37. The discussion of the balance between benefits and privacy harms with respect to the use of personal health information in support of health research provides an example of how the context can shape this analysis. *E.g.*, Fred H. Cate, *Protecting Privacy in Health Research: The Limits of Individual Choice*, 98 CALIF. L. REV. 1765, 1778–98 (2010) (describing how personal health information could aid health research and critiquing privacy-based constraints on access to that information).

38. For a thoughtful description of this type of balancing, see EUROPEAN COMM'N, TOWARDS RESPONSIBLE RESEARCH AND INNOVATION IN THE INFORMATION AND COMMUNICATION TECHNOLOGIES AND SECURITY TECHNOLOGIES FIELDS 93 (Renè von Schomberg ed., 2011), *available at* http://ec.europa.eu/research/science-society/document_library/pdf_06/mep-rapport-2011_en.pdf ("[T]he aim of any balancing is not to weigh one right against another, but more precisely, to *reconcile* the multiple values that constitute the backbone of the democratic State . . . . [T]he point of striking a balance between two values (whose antagonism might be irreducible at some point) is to preserve and enforce both of them in the best possible way.").

39. Professor Westin provided the following explanation:

> Though surveillance devices are sometimes used as a means of satisfying voyeuristic personal urges and as illegitimate weapons in political or private affairs, the more typical and important situation involves use by a public or private authority to cope with a problem of genuine social importance. . . . But if all that need be done to win legal and social approval for surveillance is to indicate a social problem and show that surveillance would help cope with it, there is no balancing at all, only a qualifying procedure for a license to invade privacy. Therefore, the need involved must be serious enough to overcome the very real risk of jeopardizing the public's confidence in its daily freedom from unreasonable invasions of privacy.

Westin, *supra* note 20, at 1206.

environmental information. Relevant context-specific considerations include what information is needed to support regulatory goals, the methods for obtaining that information, and the ultimate use of the information.

This Article begins from the premise that successful regulation of environmentally significant individual behaviors could achieve meaningful environmental benefits and argues that (1) technology is increasingly making information about individual environmental behaviors and associated harms more accessible; (2) better information about environmentally significant individual behaviors could substantially enhance fledgling efforts to regulate those behaviors; and (3) use of technology-enabled personal environmental information in support of regulation will require the resolution of myriad privacy concerns. The Article seeks to generate and inform a discussion about the appropriate balance between access to personal environmental information and privacy by identifying how regulation can benefit from personal environmental information, illustrating the trade-offs that can arise between regulation and privacy, and suggesting some initial thoughts to guide the identification and evaluation of privacy harms associated with access to personal environmental information. Part II describes how new technologies generate information about individual environmental behaviors and demonstrates how that information can enhance efforts to influence environmentally significant individual behaviors. Part III provides a preliminary overview of the privacy harms occasioned or threatened by the collection of personal environmental information. Part IV reviews some existing and proposed limits on the collection or use of personal information, motivated primarily by efforts to protect privacy in light of technological advance, to illustrate the trade-offs that can arise between regulation and privacy.

Personal environmental information could greatly aid efforts to influence environmentally significant individual behaviors, but the availability of that information depends upon successful resolution of associated privacy concerns. A failure to recognize the regulatory benefits of personal environmental information could result in privacy controls that too greatly and unnecessarily constrain access to information. A failure to recognize the privacy harms occasioned by the development of personal environmental information could not only impose unwarranted privacy harms but, once these harms are discovered, could also spur a backlash that even more greatly

constrains access to personal environmental information.[40] More generally, a failure to properly conceptualize and understand either the regulatory benefits or privacy harms associated with access to personal environmental information could lead to a suboptimal balance of access to information and privacy. Environmental scholars can contribute to debates about access to personal environmental information by explaining the potential regulatory benefits of such access and helping to understand and value associated privacy harms. The decisions that emerge will shape the technological and regulatory tools available to control individual environmental harms.[41]

II. THE PROMISE OF PERSONAL ENVIRONMENTAL INFORMATION

Adapting environmental law and policy to better and more directly address individual behavior—as opposed to the behavior of large, industrial sources of pollution—presents a significant challenge.[42] Individuals constitute a regulatory target that is notably distinct from the archetypal regulatory target in environmental law, the polluting factory.[43] Individuals are more numerous and more widely dispersed. They contribute to pollution in amounts that are often invisible at the time of release, impose harms that are frequently chronic (as opposed to acute), and become significant only when aggregated over time or with the contributions of others.[44] Individuals may also respond differently to regulatory intervention (for example, because of cognitive limitations), and government efforts to control individual behaviors may be more likely to raise objections of government intrusion.[45]

---

40. Recent legislative proposals to forbid or curtail the EPA's use of aerial surveillance to monitor compliance with environmental laws—an existing agency practice that provoked an outcry only after it was widely and erroneously publicized as being conducted using drones—provide an apt and timely example. *E.g.*, H.R. 5961, 112th Cong. (2012) ("To provide reasonable limits, control, and oversight over the Environmental Protection Agency's use of aerial surveillance of America's farmers."); *see also* David A. Fahrenthold, *Reining in the Rumor About EPA 'Drones,'* WASH. POST, June 16, 2012, http://www.washingtonpost.com/politics/reining-in-the-rumors-about-epa-drones/2012/06/16/gJQAwWjkhV_story.html.

41. Indeed, in light of the "complex nature" of the challenge of balancing technological advance and privacy, Justice Breyer "calls for resolution through a form of participatory democracy" that involves a "national conversation" conducted in part through "journal articles" and with the full participation of lawyers. Breyer, *supra* note 36, at 263.

42. Vandenbergh, *supra* note 8, at 518 ("Treating individuals as regulated entities . . . will require fundamental changes in the theories and methods of environmental law.").

43. *Id.* at 585–97 (describing the distinctive characteristics of individuals as a source category).

44. *Id.*

45. *Id.*

Lawrence Lessig offers a useful taxonomy for understanding the tools available to a modern regulatory regime when it seeks to regulate behavior.[46] He identifies four constraints that regulate behavior: law (or mandates), norms, the market, and architecture.[47] Laws, or mandates, regulate behavior by imposing requirements on behavior and providing sanctions if behavior does not heed those requirements.[48] Norms regulate behavior "not through the centralized enforcement of a state,"[49] but through expectations on behavior imposed by the community (in the case of external, or social, norms) or by individuals themselves (in the case of internal, or personal, norms).[50] Markets constrain and influence behavior through the device of price.[51] Architecture means "features of the world—whether made or found—[that] restrict and enable in a way that directs or affects behavior"[52] and includes, for example, the built environment. Architecture can thus constrain behavior by defining available transportation behaviors—it is impossible to take public transportation if none exists.

These four constraints, or modalities of regulation, "constitute the sum of forces that guide an individual to behave, or act in a given way."[53] Government can influence individual behaviors by utilizing any of these four modalities of regulation. Government can, of course, enact laws, or mandates, that directly regulate individuals by "tell[ing] individuals how they ought to behave and . . . threaten[ing] punishment if they deviate from that directed behavior."[54] It can also, however, enact laws aimed at changing norms, the market, or features of architecture that will in turn influence individual behaviors. Accordingly, government could regulate environmentally significant individual behaviors directly (through mandates) or indirectly (by

46. Lessig, *supra* note 12, at 661–72 (describing how law regulates individuals in order to explain "the project of the New Chicago School"); *see also* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 85–99 (1999).

47. Lessig, *supra* note 12, at 662–67 (identifying norms, architecture, markets, and laws as four "constraints, or modalities of regulation" that are "each *subject* to law" and proposing that "law not only regulates behavior directly, but law also regulates behavior *indirectly*, by regulating these other modalities of regulation directly").

48. *Id.* at 664.

49. *Id.* at 662.

50. Vandenbergh & Steinemann, *supra* note 9, at 1706 (describing the difference between personal and social norms).

51. Lessig, *supra* note 12, at 663.

52. *Id.*

53. *Id.*

54. *Id.* at 671.

regulating norms, the market, or architecture). This Part identifies how the regulation of environmentally significant individual behaviors using each of these modalities is being or could be enhanced by using personal environmental information generated (or potentially generated) by advances in technology.

A. Informational Regulation/Norm Management

Informational regulation and norm management may be the most promising approaches for regulating environmentally significant individual behaviors.[55] These approaches seek to provide individuals with information that persuades them to voluntarily change their behavior.[56] Individuals might voluntarily curtail environmentally harmful behaviors because they learn of previously unknown costs that the behavior imposes on them.[57] They might also change their behavior because they believe that they should (internal, or personal, norms)[58] or because they believe that society thinks that they should (external, or social, norms).[59]

The government can use information to encourage voluntary changes in environmental behaviors by influencing, or managing, the norms governing those behaviors. Technology that generates better

---

55. Dernbach, *supra* note 9, at 123–24, 132, 144; Ela, *supra* note 9, at 116–17; Vandenbergh, *supra* note 8, at 608 ("Perhaps the most important implication of the new focus on individuals as polluters is the need to look beyond the command and control versus economic incentives debate to informational regulation and norm management."). *But see* Stern, *supra* note 9, at 147–53 (identifying obstacles to changing environmental behaviors through informational regulation and norm management and observing that "[l]egal scholarship . . . has focused disproportionately on altering norms and inculcating civic virtue").

56. Vandenbergh, *supra* note 8, at 608–16 (evaluating how informational regulation can be used to influence environmentally significant individual behaviors).

57. *Id.* at 610 (using as an example that "careless use of household pesticides might change if individuals were aware that 80 percent of all pesticide exposure occurs from household pesticide use").

58. Robert Cooter, *Do Good Laws Make Good Citizens? An Economic Analysis of Internalized Norms*, 86 VA. L. REV. 1577, 1583 (2000) (characterizing a personal or internal norm as one where the individual "intrinsically values obeying a social norm [and] will pay something to obey the norm for its own sake, independent of any resulting advantage or disadvantage. In the language of economics, intrinsic value implies a 'taste' for obeying the norm."); *see also* Vandenbergh & Steinemann, *supra* note 9, at 1706 (explaining the difference between personal and social norms: "Personal norms are informal obligations that are enforced through an internalized sense of duty to act, as well as guilt or elated emotions for a failure to act.").

59. Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338, 358–66 (1997) (setting forth an esteem theory of social or external norm development); *see also* Andrew Green, *Norms, Institutions, and the Environment*, 57 U. TORONTO L.J. 105, 112–13 (2007) (assessing the potential for government to influence environmental values and norms and comparing and contrasting internal (personal) and external (social) norms).

information about individual environmental behaviors can aid norm management by educating individuals and the public about the environmental harms occasioned by individual behaviors. This can encourage the development of concrete norms against those behaviors (to the extent that the imposition of environmental harms contravenes preexisting abstract norms)[60] and facilitate the development of new or more robust social norms governing individual environmental behaviors.[61]

The environmental harms occasioned by individual behaviors are frequently difficult for individuals to recognize or comprehend.[62] This difficulty arises because: the amount of pollution or harm an individual inflicts may be unknown; an individual's contribution may cause harm only when aggregated with the contributions of others; the harms imposed by an individual may manifest at great temporal and/or geographic distance; and the causes of resulting harms, and in particular the contribution of one individual to those harms, may be unclear:

> [W]ith individuals, there are often many sources of the pollutant. . . . [E]ach release is often of a small quantity over any given time period and will only comprise a large quantity when aggregated with numerous other individual releases or when measured over a long time period. . . . [T]he release or other activity that causes the environmental harm is often not visible when caused by individuals. . . . Not only are the releases from any one individual smaller and less visible, but the harms arising from individual behavior in many cases are less visible as well. In fact, environmental harm may only arise from individual behavior when many sources are aggregated. In addition, the low concentrations and long time periods involved in many releases from individuals make it more likely that these releases will generate gradual, and in some cases almost imperceptible, changes in ecosystem health . . . . Similarly, the human health effects of many types of individual behavior are more likely to be chronic than acute.[63]

The lack of a clear connection between an individual behavior and specific environmental harm is a significant obstacle to achieving voluntary changes in behavior.[64] "[I]nformation can activate norms

---

60. *See generally* Michael P. Vandenbergh, *The Social Meaning of Environmental Command and Control*, 20 VA. ENVTL. L.J. 191, 217 (2001) ("To address second generation sources, the law could be used to tie individual actions to the environmental harms they cause.").

61. *See generally* Esty, *supra* note 10, at 190 ("Although the emergence of environmental protection as a societal goal predates the Information Age, more visible harms, information on best practices, transparency, and the democratization of decisionmaking may reinforce the inculcation of environmental values and help to speed up the norm consolidation process.").

62. Vandenbergh, *supra* note 8, at 585–96 (describing the salient aspects of environmentally significant individual behaviors and the harms that they occasion).

63. *Id.* at 589–90.

64. Technological advance may allow for better detection and understanding of the environmental harms of aggregated individual actions. Esty, *supra* note 10, at 162 (discussing how tracking the catch of fishing fleets collectively can reveal impacts on fish stocks even where

and induce behavior change if it creates a new belief that a value is threatened and that the individual can act to reduce the threat."[65] In particular, information relating to two types of beliefs may be integral for activating norms: "(1) an awareness of the consequences of the individual's act regarding the objects of an abstract norm (referred to as 'AC'), and (2) an ascription of personal responsibility for causing or preventing those consequences (referred to as 'AR')."[66] A concrete norm will develop to govern a specific behavior where individuals recognize the connection between that behavior and an abstract norm that it is designed to serve, for example, connecting the choice not to litter and environmental protection.[67] That an individual or group adheres to an abstract norm of environmental protection will do little to change a behavior that the individual or group does not understand to have a meaningful environmental consequence. Thus, for example, even if an individual possesses a strong abstract norm of environmental protection, that individual will be unlikely to adopt a concrete norm of not idling his or her car if he or she mistakenly believes that it takes more gas to turn a car off and then on than to simply idle the car.[68]

"a single fisherman or fishing boat seemingly has no effect on fish stocks"). It may also shed light on the human health impacts of pollution (the connection between a specific chemical and cancer, for example). Esty offered the following analysis:

> In combination with extraordinary new data production and collection in genomics and medicine, we stand on the verge of more scientifically robust answers to questions about how much harm pollutants cause to particular individuals. . . . The sweeping potential for improved causal specification derives not only from new analytic tools developed in the environmental field, but also from the computer-enabled knowledge revolution occurring within other disciplines, including public health, epidemiology, hydrology, statistical modeling, and risk-benefit analysis.

Id. at 158–59 (citations omitted). For example, GIS can be used to study potential links between historical environmental exposures (for example, to pesticides) and cancer. THERESA C. KENNEDY ET AL., MODELING HISTORICAL ENVIRONMENTAL EXPOSURES USING GIS: IMPLICATIONS FOR DISEASE SURVEILLANCE (2003), *available at* http://gis2.esri.com/library/userconf/health03/papers/pap3020/p3020.htm (exploring the use of GIS to track historical environmental exposures and breast cancer rates in Cape Cod).

65. Vandenbergh & Steinemann, *supra* note 9, at 1707 (describing a theory of norm development in the social psychology literature, the Values-Beliefs-Norms (VBN) theory, developed by Paul Stern and colleagues).

66. *Id.* at 1707–08 (further explaining the VBN theory).

67. For a discussion of the relationship between concrete and abstract norms, see Cooter, *supra* note 58, at 1595–96 ("Behind our particular preferences lie more general, abstract preferences."); McAdams, *supra* note 59, at 382–86 (explaining the difference between broad and narrow norms); Vandenbergh & Steinemann, *supra* note 9, at 1706 (describing "both specific, concrete norms and generalized, abstract norms").

68. Vandenbergh, Barkenbus & Gilligan, *supra* note 9, at 1725 (identifying the common "false belief[ ]" that "shutting off the engine briefly and then restarting it consumes more fuel and produces more pollution than allowing the engine to idle," explaining that restarting "consumes less fuel and emits less pollution than idling for 5 to 10 seconds," and discussing how

Similarly, even if a community possesses a strong abstract norm of environmental protection, the community will be unlikely to sanction idling (thereby supporting a concrete norm against idling) if the community mistakenly believes that it takes more gas to turn a car off and then on than to simply idle the car.

Thus, information about the connection between individual behaviors and environmental harms can be crucial for norms to spur voluntary behavior change. For example, to promote a norm of carbon neutrality, one scholar recommends the establishment of an Individual Carbon Release Inventory that would use national surveys to develop "information about the aggregate emissions attributable to individual behavior and the emissions of the average individual."[69] The scholar further posits that "[i]n addition to information about carbon emissions, individuals require information about the types of behavior changes that will generate emissions reductions, both to activate norms and provide knowledge of what steps to take once the individual feels an obligation to act."[70]

Technological advance allows for the development and communication of information that can help individuals and communities better understand the connection between their behaviors and environmental harms and thereby support the activation and development of norms governing specific, concrete individual behaviors.[71] Well-designed public information campaigns could help educate the public about the connection between certain behaviors and environmental harms and do not require access to or the use of personal environmental information.[72] However, a specific account of the harm caused by an individual enabled by access to

---

a public education campaign could be used as one element of an effort to reduce personal motor vehicle idling).

69. Vandenbergh & Steinemann, *supra* note 9, at 1729–31.

70. *Id.* at 1731.

71. For example, technology enables consumer-friendly services to compile sophisticated data about the environmental attributes of products; this can help individuals understand the environmental impacts of their consumption decisions. Robert H. Cutting et al., *Spill the Beans: GoodGuide, Walmart and EPA Use Information as Efficient, Market-Based Environmental Regulation*, 24 TUL. ENVTL. L.J. 291, 314–15, 328–29 (2011) (describing how GoodGuide "provides a user-friendly Web site and slick iPhone application that can recognize bar codes then display product information on the spot," employs Facebook and Twitter, and observing that the federal government possesses significant information about businesses and products and recommending the development and maintenance of a federal database on product and corporate environmental performance to inform consumer decisions).

72. *See, e.g.*, Gary T. Henry & Craig S. Gordon, *Driving Less for Better Air: Impacts of a Public Information Campaign*, 22 J. POL'Y ANALYSIS & MGMT. 45 (2003) (using surveys to evaluate the effectiveness of a sophisticated public information campaign designed to reduce driving and associated ozone emissions in Atlanta).

personal environmental information could prove far more powerful.[73] For example, imagine if cars periodically (daily, weekly, annually) flashed a screen detailing how the driver's behavior had wasted gas (for example, by idling or speeding) and describing the environmental impact of that wasted gas (for example, the estimated volume of associated greenhouse gas ("GHG") emissions).[74] Through "advances in the visual display of information," this information could be communicated in ways that would help overcome cognitive limitations and enable individuals to better comprehend the consequences of their actions.[75] The design of public information campaigns could also be improved by incorporating insights about individual environmental behaviors available as a result of technological advance. Imagine if GPS data could be mined to assess when, where, and why individuals in a community most commonly idle their cars. This kind of information could greatly inform the design of a public information campaign intended to reduce idling.[76]

---

73. AM. PSYCHOLOGICAL ASSOCIATIONN'S TASK FORCE ON THE INTERFACE BETWEEN PSYCHOLOGY AND GLOBAL CLIMATE CHANGE, PSYCHOLOGY AND GLOBAL CLIMATE CHANGE: ADDRESSING A MULTI-FACETED PHENOMENON AND SET OF CHALLENGES 146 (2009) [hereinafter PSYCHOLOGY AND GLOBAL CLIMATE CHANGE REPORT], *available at* http://www.apa.org/science/about/publications/climate-change.pdf (summarizing research showing that providing information that is immediate or frequent and more tailored to individual circumstances can increase the likelihood that the information will change environmental behaviors).

74. Some cars, including my own Camry Hybrid, already communicate information about how driving impacts fuel efficiency. Scott Doggett, *2012 Toyota Camry Hybrid Boosts Power and Mileage*, EDMUNDS AUTO OBSERVER (Aug. 23, 2011), http://www.autoobserver.com/2011/08/2012-toyota-camry-hybrid-boosts-power-and-mileage.html (reporting that the 2012 Camry Hybrid display screen "includes an instantaneous average mpg meter that helps motorists adjust their driving habits to achieve maximum fuel economy"). Business owners use GPS to track the fuel efficiency of their vehicle fleets, NEXTRAQ, *supra* note 7 (describing how business owners can use GPS to reduce fleet gas consumption, including by reporting on vehicle idling rates and vehicle speeds), and rental car companies have used GPS to discern when renters speed, Am. Car Rental, Inc. v. Comm'r of Consumer Prot., 869 A.2d 1198 (Conn. 2005). Eco-driving courses are offered in some EU member states and have been shown to reduce fuel consumption by ten to fifteen percent. Thomas Daniel Wuertenberger, *The Regulation of CO_2 Emissions Caused by Private Households—An Analysis of the Legal Situation in the European Union and Germany*, 16 MO. ENVTL. L. & POL'Y REV. 1, 45–46 (2009) (citation omitted).

75. Esty, *supra* note 10, at 163 (citations omitted). Esty continued:

> While no one could see the ozone layer thinning, computer-generated representations of the expanding Antarctic ozone hole helped to induce global action in response to the release of CFCs and other ozone-depleting chemicals. In fact, one of the areas of greatest promise from a more data-driven approach to environmental protection is the ability to overcome cognitive failures that have plagued problem identification and policymaking.

Id.

76. *See generally* Janet A. Weiss & Mary Tschirhart, *Public Information Campaigns as Policy Instruments*, 13 J. POL'Y ANALYSIS & MGMT. 82, 84 (1994) (identifying "captur[ing] the

Personal environmental information can also facilitate the development of new or more robust norms governing individual environmental behaviors by increasing opportunities to make those behaviors visible and comparable.[77] In this context, a behavior is visible if it can be observed or measured in some way by others.[78] Visibility of one's own behavior supports, and may be necessary for, the development of and compliance with social norms.[79] Additionally, information about the behaviors of others can influence the development of and compliance with a norm. Individuals are greatly influenced by what they perceive to be the behaviors of others.[80] For example, comparing environmental performance (between neighbors or communities) is a strategy that has proven particularly successful in spurring reductions in community and household energy use.[81]

A recent hospital study illustrates the potential for technology to increase the visibility of a behavior and to spur voluntary behavior changes as a result.[82] In an effort to encourage hand washing,

---

attention of the right audience" as crucial for the success of public information campaigns and explaining that "[c]ampaigns cannot be effective in inducing change in individuals or communities unless they are able to deliver their message to those audiences who are the targets of the campaign designers. . . . Campaign designers must know which members of the public they wish to reach and devise means to attract the notice of this audience.").

77. Notably, technology can sometimes transform into private behavior that used to be public, except for a technological information trail (for example, buying one's groceries online via FreshDirect or Peapod instead of in the full view of others at the grocery store). As one scholar observes with reference to the increasing digitization of society, "[i]ndividuals can more readily escape from the curious eyes of the community, freeing themselves from . . . social norms. . . . On the other hand, an ever-growing series of records is created about almost every facet of a person's life." Solove, *Access and Aggregation*, *supra* note 20, at 1090. On balance, however, it seems likely that technological advances will increase visibility overall with respect to many individual environmental behaviors that have heretofore often been difficult or impossible to discern. *See generally* Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 45 (2011) (comparing the privacy of purchasing a book in person and online and concluding that purchasing online allows for costless searching and distribution).

78. Ela, *supra* note 9, at 123 (describing when behavior is visible).

79. *E.g.*, McAdams, *supra* note 59, at 361–62 (setting forth an esteem theory of norm development and describing the "[i]nherent [r]isk of [d]etection" as a necessary condition).

80. Ann E. Carlson, *Recycling Norms*, 89 CALIF. L. REV. 1231, 1290 (2001); *see also* Cass R. Sunstein, *Social Norms and Social Roles*, 96 COLUM. L. REV. 903, 945 ("Experimental work shows that . . . agents are willing to cooperate, and hence to solve collective action problems without coercion, if most people are seen as cooperators.").

81. For an overview of some successful efforts to use competition to reduce energy consumption, see Hadley Rapp, Will Hoyer & Teresa Galluzzo, *Encouraging Energy Efficiency Through Competition*, IOWA POL'Y PROJECT (June 2, 2011), http://www.iowapolicyproject.org/2011Research/110602-EE-competition.html.

82. Donna Armellino et al., *Using High-Technology to Enforce Low-Technology Safety Measures: The Use of Third-party Remote Video Auditing and Real-time Feedback in Healthcare*, 54 CLINICAL INFECTIOUS DISEASES 1, 1–7 (2012); Nicholas Bakalar, *Prevention: Cameras Can*

researchers installed cameras at hand-washing sinks throughout a hospital's intensive care unit.[83] The cameras did not collect identifying personal information but did monitor workers as they entered and exited patient rooms.[84] Although workers knew about the cameras, initially only "6.5 percent washed their hands within 10 seconds of entering or leaving a room."[85] However, after researchers incorporated a feedback system in a public hallway that announced compliance rates, hand-washing rates rose to 81.6% within sixteen weeks and to 87.9% for the following eighteen months.[86] In the words of the study's lead author, "[p]eople's behavior does change when they're being watched."[87]

Presently, individual environmental behaviors, the harms that they occasion, and the precise amount of an individual's contribution to an environmental harm are often invisible, thereby preventing the comparison of individuals' environmental performances.[88] Indeed, even efforts to identify the *aggregate* environmental harms from individuals as a source, as opposed to larger industrial sources, are relatively nascent.[89] Technology increasingly permits the collection of data about individual environmental harms and allows for that data to be manipulated and disseminated. As a result of technological advance, "[w]e . . . are approaching the day when virtually all emissions will be susceptible to tagging, tracking, and measurement at relatively low cost."[90] This development can support norm campaigns by making individual harms visible and allowing for comparison:

> Data and information on what others are doing helps to define what is possible in the environmental arena. In many cases, governments, corporations, and households do not have a clear picture of what might be obtained in pollution control or resource

---

Help Ensure Hand Washing, N.Y. TIMES, Feb. 7, 2012, at D6 (describing a study reported in the journal CLINICAL INFECTIOUS DISEASES).

83. Bakalar, *supra* note 82.

84. *Id.*

85. *Id.*

86. *Id.*

87. *Id.*

88. For a critique of the "process/product" distinction that (1) can function to prevent consumer access to information about the environmental harms associated with consumption and (2) is relied upon in different areas of law and policy, see generally Douglas A. Kysar, *Preferences for Processes: The Process/Product Distinction and the Regulation of Consumer Choice*, 118 HARV. L. REV. 526 (2004).

89. For the first and most significant attempt to do so to date, see Vandenbergh, *supra* note 8, at 539–83 (defining individuals as a source category and estimating the contribution of individuals to a variety of environmental harms).

90. Esty, *supra* note 10, at 157.

> management gains. Developing good environmental metrics thus helps to clarify appropriate targets or goals. . . . [B]enchmarking opportunities may emerge at the household level. . . . Such benchmarks could provide a real spur to action at the individual level with society-wide potential for reduced pollution, especially if combined with information on how the top performers have been able to reduce their use of electricity.

Additional benchmarking gains derive from the tendency of comparative analysis, particularly rankings, to spur competition. Evidence that others are outperforming one's country, community, or company on environmental criteria can heighten attention to opportunities for improved pollution control and better resource management. Competition not only motivates better performance; it often sparks innovation.[91]

Imagine, for example, if a car not only reported the fuel impacts of a driver's driving habits but further compared the fuel efficiency of that individual's driving style to other drivers in the area.[92] Or imagine that an individual's credit card statement, or even grocery store receipt, included a consumption analysis that not only revealed the GHG emissions associated with recent purchases but also, for example, compared the GHG footprint of the individual's purchases to those of other similarly situated consumers.[93]

Better information about individual environmental behaviors, as well as more sophisticated and cost-effective methods of generating and communicating such information, thus has the potential to significantly enhance efforts to shape norms governing those behaviors. Indeed, at the broadest level, this information may help to rebut a common misconception that large industrial sources are responsible for most environmental problems.[94] Helping individuals to recognize that they are polluters and understand when and how they

---

91. *Id.* at 166–67 (citations omitted).

92. Some services already track the driving speed and distance of users to identify traffic problems and share that information with other drivers. Roy Furchgott, *Traffic Apps: Are We There Yet?*, N.Y. TIMES GADGETWISE BLOG (Aug. 21, 2009, 4:54 PM) http://gadgetwise.blogs.nytimes.com/2009/08/21/traffic-apps-are-we-there-yet/.

93. MasterCard, for example, offers a service to its corporate cardholders allowing them to automatically track and analyze carbon emissions associated with travel. Press Release, MasterCard Worldwide, MasterCard and Brighter Planet Announce New Offering to Help Companies Manage Their Environmental Footprint (May 12, 2011) (on file with author) (announcing the launch of the MasterCard Carbon Emissions Reporting feature, which provides "automatic reporting and analysis of estimated travel-related carbon emissions data . . . to corporate cardholders based on their card transactions").

94. Vandenbergh, *supra* note 60, at 198 (summarizing studies showing that much of the public mistakenly attributes a variety of environmental harms caused by second generation sources to large industrial sources of pollution).

pollute could be an important step in changing the social consequences of environmentally significant individual behaviors.[95]

B. Market

Government can also seek to influence environmentally significant individual behaviors by regulating the market (or price).[96] Government can, for example, discourage environmentally harmful conduct by raising its cost. It can impose taxes (such as a gas tax), charge for the consumption of a public environmental good (impose a usage fee), or, more indirectly, use regulation to increase the costs to produce environmentally harmful goods that firms then pass on to consumers (as through a GHG cap-and-trade program that increases the cost of energy and energy-intensive goods). Government can also encourage environmentally beneficial conduct by lowering its cost through subsidies or other means.

All of these market strategies have been or are presently used to influence environmentally significant individual behaviors, although scholars identify limitations as to each strategy.[97] Most importantly, government can't price consumption or use that it cannot quantify. It is often difficult or impossible to charge for public environmental goods or establish other market mechanisms, such as tradable allowance schemes, where millions of individuals must be regulated and the harm imposed by each is small and perhaps not subject to quantification.[98] Taxes, particularly as applied directly to individuals, are "politically radioactive" to the point that "[e]ven the strong supporters of economic measures in the academic literature have noted that the prospects for the use of taxes or fees to control pollution in the United States generally are dim."[99] Subsidies or fees may undercut efforts to use norms to promote good environmental behaviors by reducing the "green halo" effect, or the good feeling generated when an individual voluntarily makes a sacrifice in the

95. *Id.* at 215–19 (suggesting ways to change the social meaning communicated by command-and-control regulation).

96. Lessig, *supra* note 12, at 663 (describing how markets constrain individual behavior).

97. Vandenbergh, *supra* note 8, at 600–08 (critically analyzing the application of economic incentive strategies to environmentally significant individual behaviors).

98. *Id.* at 601 (identifying numerous difficulties employing market mechanisms to control individual environmental behaviors, including the expense of establishing and administering such programs, the difficulty establishing baselines and initial allocations, the low value of an allowance, and communicating unintended social meaning about polluting).

99. *Id.* at 604–05 (citation omitted).

name of environmental protection.[100] Finally, individuals do not dependably respond to price signals in expected ways, thus calling into question an assumption underlying all of these strategies, namely that increased cost will necessarily result in less environmentally destructive behavior (or vice versa).[101]

Technologically enabled increases in information about environmentally significant individual behaviors may enhance market efforts to change those behaviors in two key ways.[102] First, the information has the potential to identify, explain, and reduce errors in the establishment of price signals or consumer responses to price signals. It can thus help policymakers design market approaches that will be more effective in changing individual behaviors in desired ways. Second, this information may greatly expand the opportunities for and feasibility of charging for the consumption of public environmental goods (and establishing associated market mechanisms) by making it increasingly possible and inexpensive to track individual consumption of those goods.[103]

Policymakers struggle to determine where price signals should be set to achieve a desired amount of behavior change and resulting environmental benefit.[104] Making those predictions may be particularly fraught with difficulty when attempting to use price to influence individual behavior.[105] Better—more accurate and more immediate—information about how individuals are responding to a

---

100. Andrew Green, *You Can't Pay Them Enough: Subsidies, Environmental Law, and Social Norms*, 30 HARV. ENVTL. L. REV. 407, 432–33 (2006) ("If an individual obtains intrinsic benefits from an act, or possibly sees acting from altruism as part of her self-conception, paying her for taking the act may remove this benefit or reduce the impact of the act on her self-conception." (citation omitted)).

101. Vandenbergh, Barkenbus & Gilligan, *supra* note 9, at 1704 (describing studies suggesting that behavior does not always respond to price signals); Michael P. Vandenbergh, Amanda R. Carrico & Lisa Schultz Bressman, *Regulation in the Behavioral Era*, 95 MINN. L. REV. 715, 765 (2011) (criticizing current GHG-control strategies aimed at the household sector for "reflect[ing] strong assumptions about the influence of price and thus often overlook[ing] other influences on behavior").

102. *See generally* Esty, *supra* note 10, at 187–88 ("To the extent that information technologies ameliorate valuation disputes, make property rights easier to define and defend, and generally lower transaction costs, they eliminate a number of the obstacles that have prevented broader adoption of market-based regulatory strategies.").

103. *Id.* at 177 (describing how technology can enhance the "capacity to enforce limits on exploitation of the resource by individual actors" where resources are managed as a public good).

104. Robert R. Nordhaus & Kyle W. Danish, *Assessing the Options for Designing a Mandatory U.S. Greenhouse Gas Reduction Program*, 32 B.C. ENVTL. AFF. L. REV. 97, 146–49 (2005) (discussing the need to adjust GHG tax rates to achieve specified levels of emission reductions).

105. Vandenbergh, Carrico & Bressman, *supra* note 101, at 735–63 (explaining a variety of factors that influence individual responses to price signals).

price signal can, however, help policymakers quickly identify mistakes in pricing and make adjustments. "[R]ecently developed information and communications technologies provide a capacity to monitor market behavior on a real-time basis, including behavioral changes induced by economic incentives. By tracking activity patterns, regulators will be able to adjust tax rates to achieve optimal emissions levels."[106] Imagine, for example, that the government wished to promote sustainable fishing practices by taxing unsustainably caught fish or subsidizing sustainably caught fish. It could mine grocery records (such as online sales and sales linked to shopper discount cards) to track whether and how a change in price is changing individual purchasing decisions, including by ascertaining whether individuals who previously purchased unsustainably caught fish have switched to purchasing sustainably caught fish (or whether they are now buying hot dogs instead).[107] Quick and detailed information about how individuals respond to changed prices can, therefore, help rectify errors in setting price signals and provide greater confidence that price signals can achieve desired results.

Technology can also be used to provide individuals themselves with information about the dollar costs of their behaviors and thereby enhance efforts to use price to drive environmental behaviors. A chief concern about relying solely or primarily on price signals to change environmentally significant individual behaviors is that individuals may lack information necessary to modify their behavior in desired ways.[108] Energy pricing and energy use provide some excellent examples. Raising the cost of energy (directly or indirectly, by imposing constraints on energy producers or providers) should induce individuals to reduce energy use. However, even individuals motivated to reduce their monthly energy bill may have little concept of how to do so, let alone how to do so efficiently (i.e., by reducing energy waste while continuing valued behaviors):

---

106. Esty, *supra* note 10, at 189.

107. For a description of the information obtained by retail establishments, see Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES, Feb. 16, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_ r=1&ref=*magazine*. For a critique from a privacy perspective, see Katherine Albrecht, *Supermarket Cards: The Tip of the Retail Surveillance Iceberg*, 79 DENV. U. L. REV. 534, 534–39 (2002).

108. Vandenbergh & Steinemann, *supra* note 9, at 1725 (discussing how individuals respond to the price of electricity and concluding that "[i]ndividuals often do not have sufficient information to respond rationally to changes in price signals"). For an overview of a variety of factors, including insufficient information, that shape how individuals respond to price signals, including with respect to energy use, see Vandenbergh, Carrico & Bressman, *supra* note 101, at 743–50.

> [Individuals] tend to overemphasize the energy-reducing value of behaviors that have perceptible effects, such as turning off lights, and to discount behaviors that are less perceptible but have much greater effects on energy savings, such as improving the efficiency of heating and cooling systems. . . . One study analogized the information available to individuals when they make home energy use decisions to a grocery store in which no prices are listed on the products and the consumer receives a bill with only a total amount from the cashier.[109]

Public information campaigns can help educate consumers by, for example, explaining how various appliances and gadgets can consume energy even when not in use.[110] However, technology that reveals how a particular individual or household uses energy can offer far more nuanced and useful information to guide individuals in how to most painlessly reduce their energy use.[111] Individuals can use smart meters, home energy management systems, and smart appliances to display detailed information about their energy use in readily understandable formats, track the energy use of particular appliances, and preprogram appliances to run (or not run) at certain times depending upon electricity prices.[112] One technology proposed to aid energy conversation is an "Ambient Orb" that would glow green when a household's energy use is low but pulse red when energy use is high.[113] In this way, providing an individual with detailed information about his or her own environmentally significant behavior can reduce errors in the individual's response to price signals.

Better information about individual environmental behaviors can also greatly expand the opportunities for and feasibility of charging individuals for the consumption of public environmental goods and establishing associated market mechanisms.[114] Technology

---

109. Vandenbergh & Steinemann, *supra* note 9, at 1725.

110. *See generally* Vandenbergh, Barkenbus & Gilligan, *supra* note 9, at 1730–35 (describing energy consumption related to standby electric use and proposing a strategy for reducing that use including public education).

111. Quinn & Reed, *supra* note 16, at 870–71 (describing the benefits of smart grid data for energy conservation).

112. *E.g.*, Stern, *supra* note 9, at 146–47 (describing automated and semi-automated smart grid functions); Patrick McDaniel & Stephen McLaughlin, *Security and Privacy Challenges in the Smart Grid*, IEEE SECURITY & PRIVACY, May-June 2009, at 75–79 (describing home energy management systems); Keri Allan, *Power to the People*, ENGINEERING & TECH. MAG., Oct. 19, 2009, http://eandt.theiet.org/magazine/2009/18/power-to-the-people.cfm (describing the growing capabilities of home energy management systems).

113. THALER & SUNSTEIN, *supra* note 1, at 194 (summarizing Clive Thompson's review of Southern California Edison's creative efforts to encourage energy conservation, including the "Ambient Orb, a little ball that glows red when a customer is using lots of energy but green when energy use is modest").

114. Property or liability rules could also be established for environmental goods and applied to individuals. Vandenbergh, *supra* note 8, at 604 (describing property and liability rules, how they might be applied to individual environmental harms, and the difficulties of doing so).

is reducing "the costs of defining, protecting, and trading environmental property rights" with respect to individuals.[115] At the most basic level, technology enhances the ability to quantify the environmental harms imposed by individuals and, therefore, enhances the ability to price those harms:

> Most notably, quantitative data facilitates the "pricing" of pollution and natural resource consumption, making market-based interventions more viable. If we know how much water a homeowner has used, it is much easier to impose usage fees. And if we can measure the level of emissions coming out of a car's exhaust pipe, charging for the harm becomes much easier.[116]

A range of data about individual behaviors supports pricing the environmental goods consumed or harmed as a result of those behaviors. Already, EZ-Pass and other more sophisticated toll systems increase the feasibility of operating congestion-pricing programs.[117] (One transportation consultant predicts that smartphone technology and the cloud infrastructure will ultimately be "so precise that you will be able to charge people for how much of Fifth Avenue they use and for how long a period. In Christmas season you may decide to charge them $10 to use Fifth Avenue for each block.").[118] Smart meters and related technologies allow utility companies to track household energy use in greater detail, which in turn allows them to charge more for energy used during peak periods.[119]

The potential for attaching prices to additional harms that individuals inflict on the environment is even greater. Individual GHG

Although improved information about the harms individuals inflict on the environment, as well as new opportunities for individuals to negotiate electronically, likely makes it easier to impose some forms of property or liability rules, *see* Esty, *supra* note 10, at 175–82 (identifying how technology and better information can support property or liability rules for environmental goods), the obstacles to property or liability rules for individual environmental harms nonetheless remain daunting and for this reason are not explored in greater depth. *But see* Ostrander, *supra* note 9, at 125–33 (arguing that electronic records of purchases could be used to impose tort liability on individual consumers for the environmental harms associated with their consumption).

115. Esty, *supra* note 10, at 178.

116. *Id.* at 164–65.

117. *Id.* at 189 (observing that in Singapore "commuters pay electronically-deducted tolls with differential charges, depending on how far into the urban center they take their cars and at what time of day" and concluding that "the chance to tailor incentives with considerable precision nonetheless represents a major policy opportunity"); *see also* John Markoff, *Incentives for Drivers Who Avoid Traffic Jams*, N.Y. TIMES, June 12, 2012, at D1 (describing a program at Stanford that monitors when cars enter campus and park to reward off-peak travel). The RFID technology used to support congestion pricing was recently replaced by smartphone location data. *Id.* at D4.

118. Markoff, *supra* note 117, at D4 (quoting Samuel I. Schwartz).

119. ELLERY E. QUEEN, EDISON ELEC. INST., SMART METERS AND SMART METER SYSTEMS: A METERING INDUSTRY PERSPECTIVE 10 (2011).

emissions provide a good example.[120] The prospect of directly regulating individual GHG emissions is generally dismissed as infeasible.[121] As summarized by one scholar, rejecting as infeasible an all-source, downstream cap-and-trade program:

> Sources of CO_2, the primary GHG, number in the hundreds of millions. The sources include not only large facilities, such as those in the electricity generating sector, but also households and vehicles. The administrative costs of allowance allocation, monitoring, and enforcement for so many sources, especially the small ones, would likely be prohibitive.[122]

While a cost-effective cap-and-trade scheme incorporating all individual emissions may yet prove too unwieldy to implement, advances in estimating or tracking individual GHG emissions suggest new possibilities for pricing or otherwise regulating these emissions. Sophisticated carbon footprint calculators can generate baseline emission values by region and estimate individual emissions by looking to a variety of variables, including an individual's transportation, housing, and shopping choices.[123] Services now allow individuals to estimate the GHG emissions associated with various activities (for example, flying) and purchase carbon credits to offset those emissions.[124] This type of information can enable the pricing of

---

120. *See* Esty, *supra* note 10, at 176–77 n.214 (referencing the ability to better track greenhouse gases as an example of how information may enhance opportunities for defining property rights in environmental goods).

121. DEP'T FOR ENV'T, FOOD & RURAL AFFAIRS, SYNTHESIS REPORT ON THE FINDINGS FROM DEFRA'S PRE-FEASIBILITY STUDY INTO PERSONAL CARBON TRADING 9, 15 (2008), *available at* http://www.decc.gov.uk/assets/decc/what%20we%20do/global%20climate%20change%20and%20energy/tackling%20climate%20change/ind_com_action/personal/pct-synthesis-report.pdf (evaluating personal carbon trading and concluding that it is technologically feasible but unlikely to be cost effective: "The introduction of personal carbon trading will require a comprehensive system to assign ownership of carbon allowances to around 50 million participants, to track allowance usage by participants across all relevant retail points (petrol stations, energy suppliers, travel agents etc.) and reconcile usage against their account holdings."); Nordhaus & Danish, *supra* note 104, at 128 (describing the difficulties of implementing a downstream cap-and-trade program, applicable to all sources of GHGs including individuals). Some individuals have joined Climate Rationing Action Groups and voluntarily assumed individual carbon quotas. Sarah Krakoff, *Planetarian Identity Formation and the Relocalization of Environmental Law*, 64 FLA. L. REV. 87, 115–17 (2012) (describing Climate Rationing Action Groups).

122. Nordhaus & Danish, *supra* note 104, at 128. *See generally* Vandenbergh, *supra* note 9, at 601–02 (describing the difficulty of establishing marketable allowance schemes for individuals as polluters more generally).

123. *CoolClimate Carbon Footprint Calculator*, COOLCLIMATE NETWORK, http://coolclimate.berkeley.edu/carboncalculator (last visited Jan. 9, 2012).

124. CARBONFUND.ORG, http://www.carbonfund.org/individuals (last visited Jan. 9, 2012); TERRAPASS, http://www.terrapass.com/ (last visited Jan. 9, 2012) (allowing individuals to estimate their carbon footprint—including the carbon footprint of a wedding—and purchase

individual GHG emissions.[125] Technology makes it easier to price individual emissions both by rendering information about the volume of individual emissions more accurate and accessible and by decreasing the administrative burden posed by charging individuals for those emissions.[126]

C. Architecture

Government can also seek to influence environmentally significant individual behaviors by regulating architecture, or "features of the world" that constrain behavior or drive the harms associated with that behavior.[127] Government uses law to define architecture through zoning codes, building codes, and product mandates with significant consequences for both behavior and the environmental impacts of behavior.[128] In some instances, technology provides architecture that directly or indirectly shapes environmentally significant individual behaviors by incorporating

---

offsets for annual energy consumption, annual home energy use, annual flights, and/or annual car use).

125. Some companies now sponsor personal allowance carbon trading programs; employees use an online portal to track energy use. *See, e.g.*, *Pact at WSP*, WSP ENV'T & ENERGY, http://www.wspenvironmental.com/learnaboutus/personal-carbon-tracking (last visited July 10, 2012).

126. The Internet can allow for easier negotiation between larger numbers of people, thereby allowing for Coasian bargaining even where greater numbers of individuals are involved. Esty, *supra* note 10, at 180 ("One can imagine, for example, that property developers seeking to site a new factory may be able to negotiate electronically with the neighbors over compensation for any associated noise or dust.").

127. *See* Lessig, *supra* note 12, at 663. One critique of architectural regulation is that it can reduce transparency—individuals may not be aware of government regulation of their behavior. LESSIG, *supra* note 46, at 95–98 (describing how architectural regulation can lead to indirection); Lee Tien, *Architectural Regulation and the Evolution of Social Norms*, *in* CYBERCRIME 37, 38–46 (Jack M. Balkin et al. eds., 2007) ("[B]ecause architectural regulation regulates settings or equipment in order to regulate behavior, it changes the nature of rule presentation and rule enforcement in ways that are likely to decrease law's publicity or visibility. . . . To the extent that legitimacy and public deliberation are integral to our notion of law, the surreptitious enactment and enforcement of norms via architecture should give us pause.").

128. *See* CZARNEZKI, *supra* note 9, at 48–49, 66–68 (identifying policies that encourage individual lifestyles and decisions that are harmful for the environment, such as highway funding and agricultural subsidies). *See generally* John Turner & Jason Rylander, *Land Use: The Forgotten Agenda*, *in* THINKING ECOLOGICALLY 60, 64 (Marian R. Chertow & Daniel C. Esty eds., 1997) (describing how transportation and housing policy facilitate sprawl and associated environmental harms). Another context in which architectural regulation can regulate behavior is in the use of technology; computer code, for example, can regulate behavior. LESSIG, *supra* note 127, at 89.

automated or semiautomated features.[129] Smart appliances linked to smart meter infrastructure, for example, can "receive price signals about peak rates and remain on but automatically shift into a reduced electricity usage or conservation mode (e.g., clothes dryer will take longer to dry but the appliance is not cycled off entirely and the consumer receives discounted pricing)."[130]

Importantly, efforts to use law to define architecture in ways that change environmentally significant individual behaviors or reduce the harms arising from those behaviors require regulators to assess how existing architecture shapes behaviors and generates harms and also to predict or monitor the effects that changing architecture has on behaviors and associated harms.[131] These inquiries can prove complex; better information about environmentally significant individual behaviors may assist in generating accurate answers to both sets of questions. Urban planners and land use decisionmakers now have access to a variety of technologies—satellite map data, GIS, GPS, software—that can illuminate community behaviors and help them design and maintain local architecture.[132] GIS, for example, enables urban planners and other policymakers to link geographic information with databases to facilitate research about a variety of community conditions.[133] With

---

129. Stern, *supra* note 9, at 146–47 (describing how technology, in particular the use of automated or semi-automated features, can reduce individual environmental harms).

130. *Id.* at 146.

131. *See generally* PSYCHOLOGY AND GLOBAL CLIMATE CHANGE REPORT, *supra* note 73, at 153–54 (describing the need to accompany green architecture with psychological insights and observing that "[z]ero-energy buildings are now being developed and tested for their engineering characteristics, but if they are to approach their technical potential, they need to be designed so that occupants will not counteract the engineering, as many households now do with programmable thermostats," and that "[t]o make new designs practical and attractive, research is needed on people's responses to a new geography of communities").

132. Patricia E. Salkin, *From Bricks and Mortar to Mega-Bytes and Mega-Pixels: The Changing Landscape of the Impact of Technology and Innovation on Urban Development*, 42/43 URB. LAW. 11, 11–12 (2010/2011) (reviewing how different technologies assist urban planners); *see also Urban EcoMap San Francisco*, CONNECTED URB. DEV., http://sf.urbanecomap.org/?locale=en_US# (last visited June 25, 2012) (offering San Francisco residents an interactive website that compiles detailed local environmental data and encourages voluntary action). Connected Urban Development is an initiative that is helping localities deploy information and communications technology to reduce emissions. *Urban EcoMap: An Innovative Connected and Sustainable Cities Pilot by the Cisco Internet Business Solutions Group (IBSG) and the City and County of San Francisco*, CONNECTED URBAN DEV., http://www.cisco.com/web/about/ac79/docs/urbanecomap/factsheet.pdf (last visited Oct. 26, 2012).

133. Salkin, *supra* note 132, at 19 ("GIS has also been used for such diverse planning research as measuring crime rates in the vicinity of public housing developments, determining the location of 'food deserts,' and analyzing the effects of Census counts of prisoners on legislative redistricting and vote dilution." (citations omitted)).

respect to product mandates that set minimum standards of energy efficiency, the "rebound effect" presents a potential difficulty to predicting the effect of changing architecture.[134] Namely, when a product is more energy efficient, individuals may change their behavior to use the product more (for example, drive more when a car uses less gas) thereby reducing, nullifying, or even overwhelming any potential energy-saving gains.[135] Technology may provide ways to more readily track the response to changes in architecture, thereby allowing regulators to make adjustments that enhance environmental gains or avoid unintended environmental harms. With respect to the rebound effect, for example, smart meters can now track the energy use of some individual appliances.[136] Data could be compiled about the frequency of use of each appliance, and an increase in frequency of use, perhaps signaling a rebound effect, could be speedily detected. Thus, better information about environmentally significant behaviors can guide architecture reform to better achieve environmental protection.

D. Mandates

Government could also use law to directly impose requirements on environmentally significant individual behaviors and sanction noncompliance.[137] Mandates receive relatively little attention as a potential tool for changing environmentally significant individual behaviors primarily because enforcing mandates against millions of individuals would be costly, present administrative challenges (particularly where behaviors occur in private), and risk backlash if the public perceives enforcement as overly intrusive.[138] Moreover, it can prove difficult to generate political and public support for environmental mandates directed at individual behavior, as the costs that mandates impose on individuals—whether those costs are monetary or otherwise (inconvenience)—are generally readily

134. Nordhaus & Danish, *supra* note 121, at 157 (describing the rebound effect); Vandenbergh, Carrico & Bressman, *supra* note 101, at 738–39 (warning against overreliance on price and technology to reduce individual energy use in light of the rebound effect).

135. Nordhaus & Danish, *supra* note 121, at 157 n.229 (referencing studies showing that a ten percent increase in fuel efficiency may lead to a one percent to two percent increase in vehicle miles traveled).

136. Allan, *supra* note 112.

137. Lessig, *supra* note 12, at 664.

138. For an overview of the difficulties of applying mandates to individuals, see Vandenbergh, *supra* note 8, at 554–56, 597–600.

acknowledged.[139] Technology that enables more ready access to personal environmental information could: (1) expand the range of environmentally significant individual behaviors potentially subject to the application of a mandate by allowing for the identification of individual behaviors and associated harms; and (2) reduce the administrative burdens associated with identifying and sanctioning environmentally significant individual behaviors. As discussed *infra*, however, obtaining personal environmental information and using that information to impose mandates may engender privacy and related intrusion objections. Realizing the potential gains from personal environmental information without triggering new obstacles will thus require policymakers to tread carefully, particularly with respect to the imposition of mandates.

New technological capabilities render the application of mandates increasingly feasible with respect to many environmentally significant behaviors long viewed as beyond the scope of (feasible, cost-effective) controls. Behavior cannot be sanctioned and therefore cannot be the subject of an enforceable mandate if it cannot be identified or monitored. Additionally, the imposition of sanctions quickly becomes cost prohibitive where, as in the case of individuals, the objects of regulation number in the millions. Technology increasingly enables the identification and monitoring of environmentally significant individual behaviors in cost-effective ways;[140] it also enables cost-effective enforcement by allowing for the easy storage and manipulation of data. In the context of fisheries, for example, technology now makes it increasingly feasible to impose and enforce quotas on individual vessels:

> In combination with remote sensing, GPS and GIS technologies have the potential to improve the management of various open-access natural resources that are difficult to police. . . . To return to the problem of fisheries management, quotas can be allocated and enforced using satellite tracking to observe and even measure the number of fish being taken by particular vessels. And while the prospect of keeping track of hundreds or even thousands of fishing boats might have seemed daunting a few years ago, today's computers can manage the task with relative ease. In fact, New Zealand's fisheries recently have been revived under a tradable quota regime reinforced by a sophisticated electronic tracking system.[141]

---

139. Kuh, *supra* note 9, at 1181 (discussing how mandates reveal the costs of compliance for individuals while indirect regulation can obscure the costs that a regulatory measure imposes on individuals).

140. One program, See Click Fix, "allows people to report potholes, graffiti, and crime by uploading photos from their mobile phones. Locational information is automatically attached to the images, and local governments that team with the company receive the information directly." Salkin, *supra* note 132, at 22–23 (citation omitted).

141. Esty, *supra* note 10, at 177.

Advances in GPS, GIS, and remote-sensing technologies permit the monitoring of the catch of specific vessels and coordinating a quota system across large fleets. Household recycling behavior provides another good example of how technology can facilitate the use of mandates. Some local governments now use RFID chips embedded in recycling collection bins to help track household recycling behaviors (including everything from whether the household is recycling at all to whether its members properly separate their recyclables).[142] RFID and related software make it easier to track the recycling behavior of individual households:

> [T]he system enables the driver to communicate any issues with a particular household's recycling. The software presents a number of prompts on the CV30's touch screen, which the driver can use to note, for example, that the cart was placed backwards at the curb, or contained a large percentage of non-recyclable contaminants. The software then associates the issues with the cart ID and account information and forwards this data to the main database. Armed with this data, [the waste company or municipality] can reach out to repeat offenders and ask them to remedy the problem(s). And because the software tracks each and every cart collection, the county has been able to keep accurate records of each household's activity.[143]

Although in the example described above, the county used the collected data simply to educate households,[144] the data could also be used in support of a system of levying fines for failing to separate recyclables or otherwise comply with relevant requirements.

III. THE PERILS OF PERSONAL ENVIRONMENTAL INFORMATION: PRIVACY HARMS

Part II identified some of the potential benefits of harnessing new technology to support the regulation of individual environmental behaviors. Part III focuses on a potential difficulty posed by exploiting new technological capabilities to reveal or use personal environmental information—the privacy harms that using these technologies can occasion—and undertakes an initial effort to identify and evaluate these privacy harms. The purpose of doing so is twofold. First, privacy harms arising from access to and use of personal environmental information will likely result in the imposition of privacy-based limits on that access and use, thereby limiting, in turn, how that information can be used to support regulation. Recognizing the privacy harms and,

142. O'Connor, *supra* note 3 (describing the use of RFID tags in Charleston County, South Carolina).

143. *Id.*

144. *Id.* ("The county used this information in an education campaign in which it sent thank-you postcards to consistent recyclers and educational postcards to recycling laggards.").

as developed further in Part IV, the actual or likely privacy-based limits is thus important for presenting a fair assessment of the potential regulatory possibilities for and regulatory value of access to personal environmental information. Second, an identification and (at least preliminary) assessment of the privacy harms associated with the collection and use of personal environmental information may help in the development of privacy limits that achieve an optimal balance between the regulatory benefits of access to personal environmental information and privacy.

The development of appropriate privacy protections requires policymakers and courts to "balance privacy against countervailing interests,"[145] meaning balance the privacy harms imposed by a proposed regulation or the use of technology against the benefits of regulating (using technology) in that manner. The analysis in Part II is a first attempt to articulate one such countervailing interest by describing a benefit, namely how technology-aided identification of personal environmental harms can be used to help reduce those harms. Some value derives simply from pointing out this potential benefit. This is so because awareness of the potential value of such information can prevent the inadvertent loss of access to personal environmental information in the development of privacy policies where the information can be obtained without incurring privacy harms or where privacy harms are generally recognized as inconsequential. Defining the benefit of personal environmental information will also prove useful where obtaining personal environmental information imposes a more significant privacy harm, and the question becomes whether the benefit of the obtained information justifies imposition of that privacy harm.

Although it is perhaps more centrally the purview of privacy scholars, environmental scholars can help to conceptualize the privacy harm(s) that the benefit of developing personal environmental information is being weighed against. First, the content of the information collected, the method of information collection, and the use and disclosure of the information define the nature and extent of

145. Solove, *supra* note 35, at 483–84 (developing a taxonomy of privacy in part to assist in such balancing); *see also* Westin, *supra* note 20, at 1205–06 (proposing criteria to balance privacy and competing values in the face of new surveillance technology and observing that "achieving and maintaining a balance among the values of privacy, disclosure, and surveillance is a subtle and complicated process in every society. This is especially true in a free society seeking both liberty and stability, as well as scientific progress.").

any resulting privacy harm(s).[146] What information is collected? How? By whom? For what purpose? By identifying the type of personal environmental information needed to support policy objectives (which in turn dictates the technologies and regulation needed to obtain that information), environmental scholars can help bring into focus the privacy harms associated with obtaining that type of information. Section III.A identifies the potential privacy harms associated with some of the methods of generating and using personal environmental information described in Part II.

Second, environmental scholars can help to theorize environmental privacy more generally. For example, what rationales support recognizing privacy in personal environmental information? Are the rationales for respecting privacy weakened when an individual's actions impose externalities on others? When privacy and environmental externalities intersect, how does this shape our understanding of privacy harms? An effort to develop a theory of environmental privacy is beyond the scope of this Article,[147] but Section III.B undertakes an initial effort to frame some of the questions relevant to this larger project.

A. Identifying Privacy Harms

Extensive literatures chronicle and debate both the definition of privacy and the ways in which new technologies diminish or reshape conceptions of privacy.[148] Privacy harms that are legally cognizable (under constitutions, the common law, or statute) are a much smaller subset of the larger universe of privacy harms

146. Solove, *supra* note 35, at 485 ("The question of when and how the law should regulate [to protect privacy] can only be answered in each specific context in which the question arises.").

147. Scholars have previously analyzed privacy and environmental law in a variety of contexts but not with the purpose of developing a general theory of environmental privacy or evaluating privacy protections for environmentally significant individual behaviors. *E.g.*, Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 4, 7–11 (2006) (analyzing how environmental law and policy can provide a model for privacy regulation after the Information Revolution).

148. *E.g.*, LESSIG, *supra* note 127, at 142–56 (describing three conceptions of privacy—minimization of intrusion, protection of dignity, and substantive constraint on the power to regulate—and identifying two "distinct threats to the values of privacy" posed by technology: " 'efficient invasion': technologies now enable searching with none of the burdens that searches ordinarily entailed" and "monitoring, and the control over data that monitoring produces"); ADAM D. MOORE, PRIVACY RIGHTS: MORAL AND LEGAL FOUNDATIONS 11–32 (2010) (describing and evaluating different definitions of privacy); SOLOVE, *supra* note 20, at 131–32.

recognized by scholars and other commentators.[149] For present purposes, it is useful to focus on this latter, broader conception of privacy harms to identify the harms potentially resulting from employing new technologies to regulate environmentally significant individual behaviors. All types of privacy harms may be relevant to policymakers, courts, and citizens when weighing the benefits of using technology to generate personal environmental information against the privacy costs.

The collection and use of personal environmental information to regulate environmentally significant individual behaviors could impact a number of privacy interests. In his article, *A Taxonomy of Privacy*, Daniel J. Solove identifies and explains "privacy harms and problems that have achieved a significant degree of social recognition," with attention to privacy harms associated with new technological capabilities.[150] The following sections provide a short summary of select privacy interests adapted from Solove's categories of privacy harms,[151] accompanied by specific examples of how regulation of environmentally significant individual behaviors could implicate those privacy interests.

Information Collection[152]

Surveillance: Monitoring individuals as through visual or audio surveillance or electronic tracking.[153] *Example: A city imposes congestion pricing that is enforced primarily through the issuance of RFID tags that record the location of an individual's car at toll locations.*

Interrogation: Requesting information from individuals, even through seemingly benign questionnaires or standardized forms, where there is some onus or pressure to respond.[154] *Example: A*

149. *E.g.*, Solove, *supra* note 35, at 483 (explaining that his taxonomy of privacy harms does not simply "catalog existing laws," but "attempt[s] to understand various privacy harms and problems that have achieved a significant degree of social recognition").

150. *Id.* at 484.

151. The list includes only those privacy interests most likely to be impacted through the regulation of environmentally significant individual behaviors. Additionally, although the present use of each term largely tracks the definition offered in Solove's taxonomy, they are paraphrased, shortened, and edited to accommodate this Article's focus.

152. Notably, in addition to identifying and describing different privacy harms, Solove groups those harms into four categories: information collection, information processing, information dissemination, and invasions. Solove, *supra* note 35, at 490 fig.1.

153. *Id.* at 491–99.

154. *Id.* at 499–505.

government survey designed to estimate an individual's GHG emissions for preparation of Individual Carbon Release inventories.

Information Processing

Identification: Linking information about an individual to that person.[155] *Example: Reviewing smart meter data to characterize an individual's energy use, perhaps for the purpose of comparing the individual's energy use to that of others or educating that individual about the potential for energy savings.*

Insecurity: Collecting information about an individual that exposes that person to the risk that the information will be misappropriated, as through identity theft.[156] *Example: Using RFID tags and associated software to generate electronic records about household waste and recycling behaviors.*

Secondary use: Collecting information from an individual for one purpose and then using the information for another purpose without the individual's consent. [157] *Example: Government reviews smart meter data to monitor consumer responses to product energy efficiency mandates.*

Information Dissemination

Disclosure: Revealing true information about an individual.[158] *Example: An entity with access to household energy use data, such as the provider of software for a home energy monitor, sells that data to a marketing firm.*

Increased accessibility: Nonprivate (public) information is made more accessible to others, usually by making it available in electronic form.[159] *Example: An entity compiles publicly available data to generate estimated energy efficiency scores for homes that can be viewed on the web using the home's address.*[160]

---

155. *Id.* at 510–15.

156. *Id.* at 515–20.

157. *Id.* at 518–20.

158. *Id.* at 527–32.

159. *Id.* at 536–38.

160. Although now discontinued, Microsoft Hohm, a web-based energy management tool, performed this function:

> Based on the location of a home, we can determine numerous averages including when the year a house was built, the type of heating system, and general appliance data. . . . We calculate an estimate for your home's energy use based on public data about your

Invasion

Intrusion: Invasion of solitude, frequently as a result of information-gathering activities.[161] *Example: Installation and operation of smart meters.*

Decisional interference: Individuals' awareness of government knowledge of their behavior influences personal decisions.[162] *Example: Government uses grocery store convenience card data to monitor the impacts of a tax on unsustainably caught fish.*

These examples illustrate how different means of obtaining personal environmental information may occasion a range of privacy harms. It is also useful to recognize and further explain some factors that may exacerbate (government access to information) or mitigate (consent by the observed party) certain privacy harms and that are particularly salient for assessing the privacy harms arising from the collection and use of personal environmental information in support of regulation.

The present focus is on assessing how personal environmental information can be obtained and used to support the regulation of environmentally significant individual behaviors. As such, some government involvement in the collection or use of the information is usually anticipated. Moreover, even where government access to information is not intended, the creation of new types of personal environmental information nonetheless creates the risk of government access to that information.[163] The collection and use of personal information by the government is generally recognized to pose a threat

---

home's age, size, and structure, as well as information specific to your area, such as local weather data and common roofing materials.

See MICROSOFT HOHM, http://www.microsoft-hohm.com/Info/Help.aspx?faq=categories (last visited Apr. 17, 2012). Average or estimated energy efficiency scores were public. Once individuals joined Microsoft Hohm, they could enter specific data about their home and energy use to make the energy efficiency "Hohm Score" more accurate. *Id.* They could also elect to make their home profile public. *Id.*

161. Solove, *supra* note 35, at 548–53.

162. *Id.* at 553–58. Notably, Solove describes decisional interference as arising with respect to "those aspects of life which are socially considered to be the most private," such as decisions about "home, family, and body." *Id.* at 555. I use the term in a broader fashion to encompass less sensitive matters (such as consumption decisions).

163. *See infra* notes 180, 266, 271, 277, 281 and accompanying text (describing warrantless government access to third party records).

to liberty and occasions heightened and distinct privacy concerns.[164] As one scholar laments, "[r]ecords of personal information . . . can be used for whatever task is at hand—a tool available to anyone in power in government for use to further the current passion or whim of the day."[165] Government collection and use of information about individuals poses dangers independent of the ultimate propriety of the use for which such information is initially obtained:

> The increasing amount of personal information flowing to the government poses significant problems with far-reaching social effects. Inadequately constrained government information-gathering can lead to at least three types of harms. First, it can result in the slow creep toward a totalitarian state. Second, it can chill democratic activities and interfere with individual self-determination. Third, it can lead to the danger of harms arising in bureaucratic settings. Individuals, especially in times of crisis, are vulnerable to abuse from government misuse of personal information.[166]

As testament to the special concerns associated with government access to personal information, core statutory privacy protections focus on limiting or conditioning government access to and use of personal information.[167] Of course, the harms referenced above inhere in the government's collection of or access to personal information for any purpose, and the government already possesses a wealth of personal information about individuals.[168] That personal environmental information, like many other kinds of information, would often, by design or in effect, flow to the government should not

---

164. MOORE, *supra* note 148, at 88 (observing that "[k]eeping records of citizens has been, and continues to be, a way for governments to maintain control over their populations" and using the example of Chinese *dangan* (files) to illustrate the risk of control created by the disclosure of personal information); Schwartz, *supra* note 24, at 1633 ("From the earliest days of the Republic, American law has viewed the government as the entity whose data use raises the greatest threat to individual liberty." (citing PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 6 (1996))).

165. Solove, *Digital Dossiers*, *supra* note 20, at 1193; *see also* Balkin, *supra* note 30, at 16 ("If data mining can help us locate terrorists, why not use it to find deadbeat dads, or even people who have not paid their parking tickets?").

166. Solove, *Access and Aggregation*, *supra* note 20, at 1084–85 (internal references and citations omitted); *see also* Westin, *supra* note 20, at 1019–20, 1044 (describing the importance and role of privacy in a democratic society and observing that "one of the central elements of the history of liberty in Western societies since the days of the Greek city-state has been the struggle to install limits on the power of economic, political, and religious authorities to place individuals and private groups under surveillance against their will").

167. *E.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (2006) (placing limits on the collection, use, and disclosure of personal information by federal agencies); Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2511–20, 2701–07 (2006) (imposing limits on the government's unauthorized collection of information from modern forms of communication).

168. Solove, *Access and Aggregation*, *supra* note 20, at 1142–49, 1151–52 (describing public record-keeping and government access to personal information through the purchase of public record collections from private companies).

necessarily prevent its collection and use. For present purposes, what is important is that the potential pathologies of government access to personal information are mitigated where possible[169] and otherwise accounted for when evaluating the gravity of the privacy harms associated with the collection and use of personal environmental information.

Another important consideration when evaluating the gravity of the privacy harms associated with the collection and use of personal environmental information is how those harms might be avoided or mitigated, in particular by obtaining consent.[170] Obtaining an individual's consent can in some circumstances significantly mitigate the privacy harms associated with the collection and use of information.[171] Consent cannot, however, eliminate the privacy harms associated with the collection and use of personal environmental information. This is so because it will not be feasible to obtain consent in some circumstances without undermining regulatory aims; for consent to be meaningful, the procedures for obtaining it must be carefully designed;[172] and, even if consent is properly obtained,

---

169. Notably, the Privacy Act of 1974 incorporates Fair Information Practices and places some constraints on the collection, use, and disclosure of personal information by federal agencies, requiring, for example, that they collect only information that is "relevant and necessary" for achieving authorized purposes and disclose records only with written consent. 5 U.S.C. § 552a(b), (e). Many have, however, criticized these constraints as inadequate. *E.g.*, Solove, *Access and Aggregation*, *supra* note 20, at 1167–68 (describing how agencies can disclose information pursuant to the Act's "routine use" exception).

170. Fair Information Practices have been developed for reducing or eliminating privacy harms; one such practice is to obtain an individual's consent, where practicable, for the collection, use, or dissemination of information. ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY (2012), *available at* http://bobgellman.com/rg-docs/rg-FIPShistory.pdf (reviewing the development and describing the content of various articulations of Fair Information Practices). Consent is likely to be of particular import with respect to limiting the privacy harms associated with the collection and use of personal environmental information.

171. Professor Westin offered the following comments regarding the role of consent in defining and protecting privacy:

> Privacy means, in part, that individuals and organizations are usually permitted to determine for themselves what they want to keep private and what they want—or need—to reveal. . . . Data given to life insurance companies, credit agencies, survey researchers, or government regulatory and welfare agencies ought not be shared, in ways that identify the particular individual, without notice of the additional use and consent to it. Unless this principle of consent is understood and accepted as the first principle for controlling information flow in a data-stream society, serious problems of privacy will arise in the future.

Westin, *supra* note 20, at 1210–12.

172. *E.g.*, Cate, *supra* note 37, at 1771–78 (providing an overview of the limitations of consent, or choice, procedures and critiquing choice approaches to privacy protection in the context of health information); Schwartz, *supra* note 24, at 1661–62 (critiquing the protectiveness of consent procedures in cyberspace).

consent cannot avoid some privacy harms.[173] Consent and other practices for reducing privacy harms, while not a panacea, should be considered when designing policies for the collection and use of personal environmental information and, as with other similar practices, employed where possible to reduce privacy harms.

Serious efforts to regulate environmentally significant behaviors would benefit enormously from the input of personal environmental information; however, securing access to that information will, as the forgoing illustrates, necessarily require the navigation of a variety of privacy concerns. More detailed attention to the privacy harms associated with particular proposals for or methods of obtaining and using personal environmental information can guide the design of policies for obtaining and using such information (to minimize privacy harms where possible). Where privacy harms are unavoidable, close attention to those harms can inform consideration of and debate about balancing them with the benefits of personal environmental information.

B. Environmental Privacy

Identifying the types of privacy harms associated with the collection and use of personal environmental information does not, standing alone, suggest how those harms should be valued. The existing privacy literature houses rich accounts of the different interests in privacy and how the harms described above affect those interests, which can guide judgments about the value, or severity, of a privacy harm.[174] Surveillance, for example, can "create feelings of anxiety and discomfort," "lead to self-censorship and inhibition," and "adversely impact freedom, creativity, and self-development."[175] As

173. For example, even when information is obtained with an individual's consent, the information may remain vulnerable to misuse (insecurity).

174. Inadequate privacy protections may, for example, undermine civil society by discouraging individuals from contributing to the common good. James P. Nefh, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 1–8 (2003); Schwartz, *supra* note 24, at 1658–66 (describing constitutive privacy in the context of information use in cyberspace). With respect to individuals, inadequate privacy protections can occasion a range of dignitary and "architectural" harms that create, for example, the risk of identity theft. Solove, *supra* note 35, at 487–88 (defining and describing architectural harms to individuals); Westin, *supra* note 20, at 1022–31 (describing the "functions privacy performs for individuals in democratic societies").

175. Solove, *supra* note 35, at 493–94; *see also* MOORE, *supra* note 148, at 56 ("Having the ability and moral authority to regulate access to and uses of locations and personal information is an essential part of human flourishing and well-being. The forms of privacy may be culturally relative, but the need for privacy is not."); Westin, *supra* note 20, at 1044–47 (explaining surveillance as a means of social control and describing its effects).

explained above, government access to information presents special concerns.[176] The existing privacy literature provides substantial guidance for evaluating the gravity of particular types of privacy harms. However, a significant variable potentially useful for weighing the privacy harms associated with the collection and use of personal environmental information remains undertheorized—whether and how the value of privacy in personal *environmental* information differs from the value of privacy in other types of personal information. Although development of a theory of environmental privacy is beyond the scope of this Article, some initial thoughts follow and reveal the complexity of the inquiry. Some rationales that on first blush appear to support affording less stringent privacy protection to personal environmental information—environmental externalities imposed by individuals are in some sense public, impose harms on others, and do not constitute sensitive personal information—are less than satisfying upon closer reflection.

The secrecy paradigm, an oft-criticized but frequently used principle for recognizing and evaluating privacy harms (in particular under the common law), suggests that personal environmental information may warrant less stringent privacy protection than other types of personal information.[177] The secrecy paradigm indexes privacy protection to the extent to which information has been kept private (away from public revelation).[178] Under the Fourth Amendment, the government does not need a warrant to search an individual's garbage,[179] and, as described *infra*, the government does not need a warrant to obtain information provided by individuals to third parties.[180] Environmental externalities[181] imposed by individuals arguably fall within the heartland of information traditionally

176. *See supra* notes 20, 30, 148–62 and accompanying text (discussing the special concerns posed by government access to personal information).

177. Daniel J. Solove coined the term "secrecy paradigm" to describe a traditional approach of defining privacy as conditioned on secrecy, reflected in a variety of Fourth Amendment and tort doctrines. SOLOVE, *supra* note 20, at 42–44 ("Traditionally, privacy problems have been understood as invasions into one's hidden world. Privacy is about concealment, and it is invaded by watching and by public disclosure of confidential information.").

178. *Id.*; *see also* Solove, *supra* note 35, at 496–99 (critiquing the secrecy paradigm's failure to recognize privacy harms arising from surveillance in public spaces).

179. California v. Greenwood, 486 U.S. 35, 35 (1988) (upholding warrantless searches of garbage).

180. *See infra* notes 271–72 and accompanying text (explaining the third party doctrine).

181. A (negative) environmental externality is simply a harm to the environment that an individual inflicts but does not pay for. For a more nuanced exploration of the definition of environmental externalities, see Ezra Rosser, *Offsetting and the Consumption of Social Responsibility*, 89 WASH. U. L. REV. 27, 32–33 (2011).

understood to be public under the secrecy paradigm. Just like garbage, emissions or other externalities released by individuals directly into the environment are in some sense exposed to others and therefore not secret. Thus, with respect to many ways that individuals harm the environment, claims to privacy as to, for example, the identity of the emitter or the volume or substance of emissions released, are arguably weak because, by definition, an externality is in some way public and not secret.

However, a number of further considerations complicate reliance on the secrecy paradigm to justify limiting privacy protections for personal environmental information. First, as described *infra*, many scholars and some courts criticize the secrecy paradigm for failing to adequately protect significant privacy interests, particularly in light of technological advance.[182] Additionally, the secrecy paradigm does not map neatly onto some means of obtaining personal environmental information. Technology may, for example, make previously invisible externalities visible, such as remote sensors that analyze tailpipe emissions from passing cars.[183] When individuals release substances into the environment that are only visible using specialized equipment are those releases public or private?[184] Moreover, in many circumstances, identifying the environmental externalities imposed by an individual may require tracking behavior from which the externality can be extrapolated. For example, individuals indirectly impose many environmental externalities (such as GHG emissions) through their consumption of goods and services (such as energy).[185] To identify these indirect externalities, regulators

182. *See infra* notes 264, 278–80 and accompanying text (describing critiques of the third party doctrine and the secrecy paradigm).

183. U.S. ENVTL. PROT. AGENCY, EPA 420-F-92-017, REMOTE SENSING: A SUPPLEMENTAL TOOL FOR VEHICLE EMISSION CONTROL 1 (1993) ("Remote sensing is a way to measure pollutant levels in a vehicle's exhaust while the vehicle is traveling down the road.").

184. Perceptions of the visibility of information can shape expectations of privacy. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding the use of a thermal-imaging device to detect heat patterns within a home constituted a Fourth Amendment search requiring a warrant).

185. For an overview of the environmental impacts of consumption, see Salzman, *supra* note 9, at 1249–51 ("In regard to the environmental impacts of commercial energy consumption, for example, the average African family would need to bear more than ninety children to equal the impact of an American couple with only two children." (citation omitted)). *See also* Albert C. Lin, *Virtual Consumption: A* Second Life *for Earth?*, 2008 BYU L. REV. 47, 53–61 (2008) (describing the environmental impacts of consumption). For a nuanced analysis of the consumer's contribution to the environmental harms occasioned by the production of consumer goods, see Rosser, *supra* note 181, at 36–41 ("Consumers do not merely buy the end product; they also have indirect ownership over the process that created the product. If all I do is buy a pair of shoes produced through exploitation of workers or destruction of the environment, I am participating in the harm.").

must extrapolate environmental harm from individual consumption.[186] While consumption is often public, the environmental externalities associated with consumption are frequently invisible.[187] Thus, it is not immediately clear whether individual environmental externalities fall within the scope of the secrecy paradigm; moreover, the justifications for using the secrecy paradigm to define privacy protections are increasingly questioned.[188]

Another rationale for limiting the privacy afforded to personal environmental information stems from the fact that such information usually identifies externalities (direct or indirect) imposed by individuals on others. Even where claims to privacy are strong because of the context (for example, the conduct occurs in a private home)[189] or the sensitivity of the information involved (for example, personal medical information[190]), privacy interests may be subordinated where an activity harms another or divulgence of information is necessary to avoid harms to others.[191] When

186. The meaning and significance of consumption to individuals is complex and disputed. *See* Lin, *Virtual Consumption*, *supra* note 185, at 62–73 (explaining different theories of consumption).

187. *See generally* Kysar, *supra* note 88, at 536–37 (describing American consumers' "institutionalized ignorance" about the production processes of products they consume).

188. *E.g.*, MOORE, *supra* note 148, at 19–20 (criticizing definitions of privacy resting on a public/private distinction because of technology's ability to publicize previously private behaviors). "[T]he availability of information is dependent upon technology. Telescopes, listening devices, heat-imaging sensors, and the like open up what most would consider private domains for public consumption. What we are worried about is what *should* be considered a 'private affair'—something that is no one else's business." *Id.* (emphasis in original).

189. Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV. 905, 912–20 (2010) (describing and critiquing heightened privacy protections afforded within the physical home).

190. Ferguson v. City of Charleston, 532 U.S. 67, 83–84, 84 n.21 (2001) (distinguishing roadblock seizures as less intrusive than body searches and holding that the unauthorized dissemination of diagnostic test results constitutes an unreasonable search).

191. *Compare* Osborne v. Ohio, 495 U.S. 103, 109–11 (1990) (upholding an Ohio law forbidding the possession and viewing of child pornography because it was "enacted . . . to protect the victims of child pornography; it hopes to destroy a market for the exploitative use of children."), *with* Stanley v. Georgia, 394 U.S. 557, 564–68 (1969) (striking down a Georgia law forbidding the possession of obscene materials and emphasizing the privacy and sanctity of the home). *See generally* Whalen v. Roe, 429 U.S. 589, 602–04 (1977) (upholding a New York statute requiring that the state be provided with prescriptions for certain drugs against a privacy challenge and observing that "disclosures of private medical information . . . to public health agencies are often an essential part of modern medical practice even when the disclosure may reflect unfavorably on the character of the patient. Requiring such disclosures to representatives of the State having responsibility for the health of the community, does not automatically amount to an impermissible invasion of privacy."); Tarasoff v. Regents of the Univ. of Cal., 551 P.2d 334, 347–48 (Cal. 1976) (holding that therapists have a duty to reveal confidential information about a patient where the patient presents a serious danger of violence to another and observing that "the public policy favoring protection of the confidential character of patient-

aggregated, individual environmental behaviors generate staggering environmental and related human harms;[192] this perhaps suggests a basis for limiting privacy protections for individual environmental externalities.

However, as with the secrecy paradigm, application of this principle to personal environmental information is not straightforward. Many of the prior examples where privacy is subordinated are distinguishable because the harm at issue is more significant, the need for the information to prevent or redress the harm is clearer, or the individual whose privacy is compromised plays a more substantial or active role in creating the harm. Most harms that individuals impose on the environment are relatively small (and only impact others when aggregated over time or with the harms of others), and the contribution of an individual's action to a specific environmental or human health manifestation of harm is likely to be difficult if not impossible to establish. Many harms that individuals impose on the environment arise as a result of common, everyday behaviors that may be unknown to the individual or unavoidable, and the environmental harms that result may be widespread and may impact the emitting individual as well.[193] Moreover, because they frequently involve common behaviors, a decision to subordinate privacy with respect to personal environmental information will likely affect everyone. As such, the privacy considerations with respect to individual environmental externalities may be more akin to those that arise with respect to other common behaviors subject to broad regulation that have small, incremental effects on the public good such as, for example, requirements to divulge information on tax forms.[194] Thus, further thought is needed to discern whether or how the general principles that support subordinating privacy with respect to harmful externalities might apply to personal environmental information.

---

psychotherapist communications must yield to the extent to which disclosure is essential to avert danger to others. The protective privilege ends where the public peril begins."); Helena Gail Rubinstein, *If I Am Only for Myself, What Am I? A Communitarian Look at the Privacy Stalemate*, 25 AM. J.L. & MED. 203, 227 (1999) ("Privacy concerns are subsumed to the community benefit in cases of communicable disease, where notification is required by law. Communities are notified when a sexual predator takes up residence in the area. The balance in these cases resides with the community, not the individual." (citations omitted)).

192. *See* Vandenbergh, *supra* note 8, at 545–84 (documenting the volume of individual contributions to a number of environmental problems).

193. *See supra* notes 150–62 and accompanying text (describing the nature of and challenges for regulating environmentally significant individual behaviors).

194. *See generally* William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1029–34 (1995) (describing the ways in which regulatory regimes routinely and necessarily require access to private information to function).

Finally, it could be claimed that personal environmental information, as a category of information, is not particularly sensitive or central to personal dignity, autonomy, personhood, etc., and is thus less deserving of strong privacy protections. The volume of pollutants in an individual's tailpipe emissions or home lawn pesticide applications, for example, hardly seems particularly consequential. However, while on the surface the characterization of personal environmental information as low value (from a privacy perspective) may have some appealing logic, this claim, too, becomes complicated on further reflection. Even if the relevant personal environmental information itself is not sensitive (for example, the externalities associated with an individual's consumption),[195] the means needed to obtain it may require divulging more sensitive information (such as consumption choices) or using surveillance, monitoring, or other mechanisms that independently inflict privacy harms.

The discussion above identifies some considerations that may prove relevant to assessing the strength of claims to privacy for personal environmental information. Developing a more robust theory of environmental privacy will require deep engagement with privacy theory and is beyond the scope of this Article.[196] Developing such a theory is, however, a task that scholars should embrace. A thoughtful theory of environmental privacy that assigns value to the types of privacy harms most often associated with the development of personal environmental information and critically examines rationales for limiting or protecting the privacy of personal environmental information would prove a useful tool as scholars and policymakers navigate advances in technology and privacy concerns in the effort to reduce individual environmental harms.

---

195. One commentator has argued that society should afford little privacy to consumption with environmental impacts:

> Privacy, especially in the domain of consumption, may have the appearance of tangible meaning, but upon further examination, it breaks down into little more than an empty cocoon that is a mere metamorphic remnant in the process of technological and social evolution. . . . In sum, while technological hurdles and privacy-based concerns will function as impediments to determining who buys what, in time we can expect these obstacles to diminish.

Ostrander, *supra* note 9, at 128.

196. These preliminary thoughts may provide a useful starting point for fully engaging the privacy literature and recognizing the complexities that exercise will present.

IV. ILLUSTRATING TRADE-OFFS: HOW PRIVACY-DRIVEN LIMITS ON EMERGING TECHNOLOGIES CAN CONSTRAIN THE REGULATORY POTENTIAL OF PERSONAL ENVIRONMENTAL INFORMATION

This Part provides examples of existing and proposed limits on the collection or use of personal information, motivated primarily by efforts to protect privacy in light of technological advance, that illustrate how such limits could constrain the use of personal environmental information to regulate environmentally significant individual behaviors. Specifically, privacy concerns are shaping the deployment and use of RFID and smart meter technology. Technological advances are also inspiring courts to consider narrowing the scope of the third party exception to the Fourth Amendment. These developments, surveyed below, illustrate how privacy concerns can shape the deployment and use of new technologies—as well as access to the information those technologies generate—impacting the utility of those technologies for regulating environmentally significant individual behaviors. Of note, this survey should not be taken as a critique of the need for privacy protections generally or of the specific privacy protections reviewed.[197] The purpose here is simply to provide some examples of trade-offs between access to personal environmental information to support regulation and privacy as privacy protections are applied to new technologies. The larger goal is to help inform optimal balancing of access to information and privacy; one aspect of this is understanding trade-offs—how privacy protections can define regulatory benefits.

A. Radio Frequency Identification

RFID technology may have numerous applications useful for identifying individual environmental harms. Already, RFID facilitates

197. Indeed, many scholars and advocacy groups lament the lack of more stringent privacy protections; the United States generally emphasizes private-party self-regulation and the need to shelter emerging technologies from unnecessary restraints. *See* Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 232 (1999) (explaining the United States prefers individualized citizen-based information privacy control over centralized government-based regulation); Jonathan Collins, *Rep. Senators Vow to Protect RFID*, RFID J. (Mar. 10, 2005), http://www.rfidjournal.com/article/articleview/1440/1/ (quoting the Senate Republican High Tech Task Force's intention to " 'protect exciting new technologies from premature regulation or legislation in search of a problem. RFID holds tremendous promise for our economy, including military logistics and commercial inventory efficiencies, and should not be saddled prematurely with regulation.' ").

the implementation of congestion-pricing[198] and recycling programs;[199] future applications may shed further light on environmentally significant individual behaviors and thereby enable or facilitate their regulation.[200] However, as advocacy groups,[201] scholars,[202] and the

198. *See supra* notes 117–18 and accompanying text (describing RFID's use in congestion-pricing programs as a market mechanism for regulating environmentally significant individual behavior).

199. *See supra* notes 142–44 and accompanying text (describing the use of RFID in recycling collection).

200. A proposed but now-inactive bill in California would have authorized local governments to "participate in a local traffic safety program that uses radio frequency identification (RFID) technology in order to aid law enforcement efforts, promote environmental initiatives, including congestion mitigation, and enhance revenue collections of unpaid fines and penalties." S.B. 767, 2011–2012 Leg., Reg. Sess. (Cal. 2011). RFID may also support monitoring of extended-producer responsibility policies designed to increase consumer electronics recycling. LARS THOROE ET AL., RFID-BASED INDIVIDUALIZATION OF EXTENDED PRODUCER RESPONSIBILITY AND RECYCLING FOR WEE (2011), *available at* http://aisel.aisnet.org/ecis2011/106. And RFID may be used to track trash and shed more light on product life cycles. Jennifer E. Smith, *You Can Run, But You Can't Hide: Protecting Privacy from Radio Frequency Identification Technology*, 8 N.C. J.L. & TECH. 249, 262–63 (2007) (describing "a patent entitled Radio-frequency tags for sorting post-consumer items, which outlines a plan to compile and sell data on consumers' trash," creating the possibility that "the entire life cycle of an item may be tracked" (internal quotation marks omitted)). RFID is also being used to monitor and enforce parking rules, as well as "helping to understand parking behavior, and residents' travel habits." Laura M. Ulatowski, *Recent Developments in RFID Technology: Weighing Utility Against Potential Privacy Concerns*, 3 I/S J.L. & POL'Y 623, 631–33 (2008) (describing how Hoboken officials installed RFID chips in parking permits to aid in parking enforcement and are using the generated information for various "good reasons," but observing that "[r]esidents . . . might be worried that they will lose their anonymity" (citing Renee Boucher Ferguson, *City of Hoboken Using RFID in Parking Permits*, EWEEK.COM (June 12, 2006), http://www.eweek.com/article2/0,1759,1975813,00.asp)). RFID may also be used to support ecological labeling, allowing consumers to scan products to learn their environmental attributes. Cutting et al., *supra* note 71, at 313 ("Information, such as the carbon footprint of the product, whether it is a recycled product, precise ingredients, or whether it is organic or sustainable in some other way, appears right on the label. Given that radio frequency identification (RFID) technology is already here, why not encode current information on the company and product into the chip so it can be read by the consumer?").

201. For an example of the concerns of privacy advocacy groups about RFID, see PRIVACY RIGHTS CLEARINGHOUSE, RFID POSITION STATEMENT OF CONSUMER PRIVACY AND CIVIL LIBERTIES ORGANIZATIONS (2003), *available at* http://www.privacyrights.org/ar/RFIDposition.htm (issued by, among others, the American Civil Liberties Union, Electronic Frontier Foundation, and Electronic Privacy Information Center; identifying how RFID can invade privacy and contrasting acceptable uses of RFID with uses that "[s]hould be [f]latly [p]rohibited").

202. *See* Laura Hildner, *Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. C.R.-C.L. L. REV. 133, 168–71 (2006) (advocating for state RFID restrictions); Smith, *supra* note 200, at 257–66 (exploring the privacy implications of RFID technology); Ulatowski, *supra* note 200, 627–47 (reviewing applications of RFID technology and identifying associated privacy concerns); Stein, *supra* note 23, at 1, 20–22 (proposing federal regulation of RFID to protect privacy).

public[203] have all opined, RFID technology raises myriad privacy concerns that are shaping the deployment of it.[204] At the federal level, arguments for restraint to allow time for the technology to develop and for industry self-regulation have largely prevailed.[205] States have, however, been quicker to impose privacy-driven constraints on the use of RFID technology.[206] State limits on RFID technology include those focused on specific uses of RFID—barring or imposing conditions on the use of RFID in driver's licenses or other state-issued identification documents,[207] barring the required implantation of an RFID device,[208] criminalizing the use of RFID technology to commit fraud or identity theft[209]—as well as more general laws prohibiting how information

---

203. "The most significant concerns expressed by consumers familiar with RFID related to privacy. . . . Many of those consumers voiced strong opposition to having RFID devices track their purchases and movements, with some citing as reasons for their position the potential for increased marketing or government surveillance." FED. TRADE COMM'N, RFID: APPLICATIONS AND IMPLICATIONS FOR CONSUMERS 12–13 (2005) (reporting the results of a public survey revealing significant public concern about how RFID can invade privacy).

204. K. MICHAEL & L. MCCATHIE, INT'L CONFERENCE ON MOBILE BUS., THE PROS AND CONS OF RFID IN SUPPLY CHAIN MANAGEMENT 623–29 (2005), *available at* http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1104&context=infopapers ("Privacy issues loom as one of the biggest threats to the unbridled success of RFID. Privacy concerns have the potential to 'stop a technology dead in its tracks.' " (citation omitted)).

205. *See* Hildner, *supra* note 202, at 167–68 (concluding that the "odds of passage are poor" for federal RFID-specific privacy legislation); *see also* FED. TRADE COMM'N, *supra* note 203, at 21–23 (concluding that industry self-regulation is appropriate to address RFID-related privacy concerns). Congress, for example, requires that state driver's licenses and identification cards meet federal minimum requirements to be accepted for certain official purposes; one such requirement is that licenses or identification cards include "[a] common machine-readable technology, with defined minimum data elements." Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Pub. L. No. 109-13, § 202, 119 Stat. 231, 312–15. RFID would satisfy that technology requirement; *see* 6 C.F.R. § 37.19 (2012) (specifying minimum technical requirements). RFID is also used to facilitate border crossings, including in enhanced driver's licenses issued by some states. Documents Required for Travelers Departing From or Arriving in the United States at Sea and Land Ports-of-Entry From Within the Western Hemisphere, 73 Fed. Reg. 18,384, 18,390, 18,395 (Apr. 3, 2008).

206. The National Conference of State Legislatures has compiled a chart of state-level RFID privacy measures. *State Statutes Relating to Radio Frequency Identification (RFID) and Privacy*, NAT'L CONF. OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/radio-frequency-identification-rfid-privacy-laws.aspx (last visited May 15, 2012).

207. *E.g.*, ARK. CODE ANN. § 27-16-1206 (West 2012) ("The Office of Driver Services of the Department of Finance and Administration shall not include an electronic chip or any type of radio frequency identification (RFID) tag or chip in any driver's license or identification card or enhanced security driver's license or identification card issued by the Department of Finance and Administration.").

208. *E.g.*, N.D. CENT. CODE ANN. § 12.1-15-06 (West 2012) ("A person may not require that an individual have inserted into that individual's body a microchip containing a radio frequency identification device.").

209. *E.g.*, NEV. REV. STAT. ANN. § 205.46515 (West 2012) ("A person shall not knowingly, intentionally and for the purpose of committing fraud, identity theft or any other unlawful act:

can be obtained using RFID or how RFID-obtained information can be used.[210] Restrictions on how commercial entities can use RFID tags in stores and consumer products have also been proposed.[211]

Although state restrictions on RFID are not aimed specifically at limiting the use of the technology to obtain personal environmental information, some state law restrictions are broad enough to potentially frustrate such efforts. In New Hampshire, the state and its political subdivisions may not use RFID to determine the ownership of a car or the identity of persons within a car "on the public ways of the state or its political subdivisions," except in certain enumerated circumstances.[212] In Rhode Island, personally identifiable information from RFID-equipped toll devices is not considered public and can be "released to law enforcement agencies only for: (1) toll enforcement purposes; or (2) for other purposes if accompanied by a court order."[213] Washington state issues RFID-equipped identification cards.[214] However, it is a felony to read information on another person's identification document, except in a small number of enumerated circumstances (including where the document is read "in the course of a good faith security research, experimentation, or scientific inquiry including, but not limited to, activities useful in identifying and analyzing security flaws and vulnerabilities.").[215] In Washington,

---

(a) Capture, store, or read information from the radio frequency identification document of another person without that other person's knowledge and prior consent . . . .").

210. *E.g.*, N.H. REV. STAT. ANN. § 236:130 (2011) (forbidding any state actor from using RFID technology to determine a motor vehicle's ownership or the identity of its occupants); R.I. GEN. LAWS ANN. § 42-153-4 (West 2012) (restricting the state's use of toll payment information obtained by RFID tags to "toll enforcement purposes" or "other purposes if accompanied by a court order").

211. *E.g.*, S.B. 1850, 187th Gen. Ct. § 3 (Mass. 2011) (proposing to require commercial entities to notify consumers of RFID systems and label products using an RFID tag); Assemb. B. 1732, 214th Leg., 2010. Sess. § 2 (N.J. 2010) (proposing to require businesses using RFID tags to notify customers, label products, and detach RFID tags upon purchase); Assemb. Bill 1033, 2011 Leg., Reg. Sess. (N.Y. 2011) (proposing to require notification, labeling, and the removal of RFID tags at the point of sale; further prohibiting the aggregation of personal information and RFID tag information, the sale of RFID-generated personal information to third parties, and the use of RFID identification tags to identify a customer). Similar federal legislation has also been proposed. Opt Out of ID Chips Act, H.R. 4673, 108th Cong. (2004) (as referred to the Subcommittee on Commerce, Trade and Consumer Protection).

212. N.H. REV. STAT. ANN. § 236:130. Exceptions include where surveillance is "specifically authorized by statute" or "undertaken for purposes of operation of the E-Z Pass system . . . ." § 236:130(III).

213. R.I. GEN. LAWS ANN. § 42-153-4.

214. WASH. REV. CODE ANN. § 46.20.202 (West 2012) (authorizing the issuance of enhanced drivers' licenses and "identicards").

215. WASH. REV. CODE ANN. § 9A.58.020 (West 2012). California imposes a similar restraint. *See* CAL. CIV. CODE § 1798.79(a), (e) (West 2012) (criminalizing "intentionally remotely read[ing]

personally identifying information from identification cards or RFID-enabled toll collection can only be released in aggregate form or "to law enforcement agencies only for toll enforcement," for "United States customs and border protection enforcement purposes," or pursuant to court order.[216] Additionally, governmental and business entities are barred from reading commercial RFID-identification devices that they did not issue except in certain limited circumstances (including, again, an exception for "[r]emotely reading or storing data from a person's identification device in the course of an act of good faith security research, experimentation, or scientific inquiry.").[217]

These laws, and others like them,[218] could complicate use of RFID in support of congestion pricing, to enforce speed limits or anti-idling laws, or to develop better information about individual environmental behaviors to enhance the design of policies targeted at those behaviors. For example, in New Hampshire, a city would not be permitted to issue parking permits equipped with RFID; Hoboken, NJ is already using such a system to better understand and manage parking demand.[219] Notably, in contrast to the experience with smart meters, where at least some potential environmental applications are widely recognized and privacy protections have been evaluated with an eye to preserving those applications, the potential benefits of RFID for regulating environmentally significant individual behaviors do not appear to be widely recognized or taken into account in crafting RFID privacy measures.

B. Smart Meters

Concerns about the way in which smart meters and related advanced metering technologies may invade privacy are informing the

---

or attempt[ing] to remotely read a person's identification document using radio frequency identification . . ." without that person's consent; exempting use of such information for "good faith security research, experimentation, or scientific inquiry").

216. WASH. REV. CODE ANN. § 42.56.330 (West 2012).

217. WASH. REV. CODE ANN. § 19.300.030 (West 2012).

218. Vermont prohibits the compilation of "a database of electronically readable information derived from" driver's licenses or other state identification cards; however, the prohibition does not apply to the use of such a database "for . . . government purposes," and likely permits government collection and use of personal environmental information for regulatory purposes. VT. STAT. ANN. tit. 23, § 7 (West 2012); *see also* CAL. PENAL CODE § 637.7 (West 2012) ("No person or entity in this state shall use an electronic tracking device to determine the location or movement of a person.").

219. *See supra* note 200 (describing Hoboken's RFID parking permit program).

design and deployment of smart meters.[220] In contrast to RFID, at least one potential environmental application of smart meters—providing individuals with access to their own electricity use data in support of conservation efforts—features prominently in the contemplation of appropriate privacy protections,[221] which generally seek to preserve that core function of smart meters.[222] Companies are rapidly developing a variety of programs to provide energy consumption data to individuals in an accessible, thoughtful format that enables and incents conservation behaviors.[223] This capacity is frequently recognized as justification for and a benefit of the deployment of smart meters;[224] policymakers crafting privacy protections for smart meters have recognized and largely preserved this smart meter function, although, as shown below, privacy policies nonetheless impose some constraints on the potential for smart meters to support voluntary energy conservation.[225]

Government access to smart meter data could also support the regulation of environmentally significant individual behaviors by, for example, allowing for the detection of rebound effects or, more generally, providing detailed data about energy use behaviors to

---

220. *E.g.*, NAT'L ASS'N OF REGULATORY UTIL. COMM'RS, RESOLUTION ON SMART GRID PRINCIPLES 1–2 (2011), *available at* http://www.naruc.org/Resolutions/Resolution%20on%20Smart%20Grid%20Principles.pdf; NAT'L INST. OF STANDARDS & TECH., NIST IR 7628, GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 2, PRIVACY AND THE SMART GRID 1–42 (2010), *available at* http://csrc.nist.gov/publications/PubsNISTIRs.html; NAT'L ASS'N OF STATE UTILS. CONSUMER ADVOCATES, RES. 2009-03, SMART GRID PRINCIPLES OF THE NATIONAL ASSOCIATION OF STATE UTILITIES CONSUMER ADVOCATES ¶ 9 (2009), *available at* www.nasuca.org/archive/2009-03%20FINAL.doc. Often these discussions center on how best to incorporate the *Fair Information Practices Principles*, FED. TRADE COMM'N, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited Sept. 1, 2012), into the Smart Grid. *See, e.g.*, NAT'L ASS'N OF REGULATORY UTIL. COMM'RS, *supra*, at n.2 (using Fair Information Privacy Principles as resource for "privacy policies").

221. QUINN, *supra* note 18, at v–vii.

222. *See supra* notes 15–16 and accompanying text (explaining how smart meter data can educate consumers and help achieve voluntary reductions in energy consumption).

223. Some utility providers are working with companies to incorporate that functionality into the base smart meter service; other companies market these programs directly to consumers. Quinn & Reed, *supra* note 16, at 876–79 (describing "edge service providers who have cropped up to manipulate and present electricity usage data at the edge of the electricity network").

224. *But see id.* at 842–43 (explaining why utilities may not provide full support to such non-traditional functions of smart meter technology).

225. QUINN, *supra* note 18, at 9–16 (recognizing that "[t]he threshold motivation behind smart grid deployment is to enable environmentally sensitive electricity generation, distribution, and consumption practices"; reviewing privacy concerns; and discussing how privacy regulation might impact the function and value of smart meters).

inform energy conservation policies.[226] For the reasons described above, however, government access to smart meter data presents serious privacy concerns.[227] Interestingly, in spite of the gravity of the privacy concerns at stake, government access to smart meter data, as compared to access by private third parties, appears to have received relatively less attention in discussions about smart meter privacy.[228] This raises two concerns. Although unfettered government access to smart meter data seems unlikely and ill-advised, some government access for environmental purposes, structured in ways to mitigate privacy harms, could, if carefully designed, prove both useful and feasible. Possibilities for such access could be frustrated by the adoption of privacy policies developed without recognition of the need to preserve or facilitate such access. More likely, however, if no or inadequate restrictions on government access are in place, justifiable privacy concerns could occasion a backlash resulting in overly broad restrictions on government access that would preclude even limited access structured with safeguards against misuse.[229]

---

226. *See supra* notes 134–36 and accompanying text (describing how smart meter data could be used to support market regulation of individual environmental behaviors by detecting rebound effects); *see also* LOCAL GOV'T SUSTAINABLE ENERGY COAL, COMMENTS OF THE LOCAL GOVERNMENT SUSTAINABLE ENERGY COALITION ON PROPOSED DECISION ADOPTING PRIVACY RULES 1–2 (2008), *available at* http://docs.cpuc.ca.gov/efile/CM/136530.pdf (Pub. Utils. Comm'n of the State of Cal. Rulemaking No. 08-12-009) (explaining the need for local government access to smart meter data in support of greenhouse gas emission reduction programs). For a discussion of potential statutory and constitutional restrictions on government access to smart meter data, see *infra* notes 265–77 and accompanying text (discussing the applicability of warrant requirements to smart meter data).

227. *See supra* notes 20, 30, 148–62 and accompanying text (describing the special privacy concerns occasioned by government access to personal information).

228. *See* McNeil, *supra* note 18, at 202 (observing that law enforcement access to smart grid data has "received relatively little attention" and suggesting this may be the result of a lack of understanding of smart meter technology). Attention to government access to smart meter data has focused largely on law enforcement use of smart meter records to detect, for example, marijuana growing operations and whether or how such law enforcement access would be subject to Fourth Amendment protections and/or federal statutory privacy requirements. *E.g.*, BRANDON J. MURRILL, EDWARD C. LIU & RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R42338, SMART METER DATA: PRIVACY AND CYBERSECURITY 7 (2012) [hereinafter CRS SMART METER PRIVACY REPORT] (noting that "[t]he use of smart meters presents the recurring conflict between law enforcement's need to effectively investigate and combat crime and our desire for privacy while in our homes" and analyzing the propriety of access to smart meter data for government investigations); McNeil, *supra* note 18, at 205–06.

229. Some empirical data suggests that individuals view government access to electricity records as relatively intrusive. Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 333–36 (2008) (reporting the results of an empirical study in which individuals ranked government conduct by level of intrusiveness; access to electricity records was ranked eleventh out of twenty-five scenarios).

At present, it is primarily state public utility commissions that are developing and imposing smart meter privacy protections.[230] Some state public utility commissions require that consumers be allowed to "opt-out" and not use smart meter technology (in part out of deference to customer privacy concerns);[231] public utility commissions have also adopted new privacy policies aimed specifically at smart meter technology.[232] Together, these developments can affect the use of smart meter information to regulate environmentally significant individual behavior by (1) directly limiting the deployment of the technology as a result of customer opt-out; (2) directly or indirectly[233] shaping access by environmental agencies to smart meter data; and (3) imposing barriers to the development and use of home energy management systems.

1. Customer Opt-Out

Many individuals express concern about the private information that smart meter data can reveal and about access to and use of that data.[234] Some utility customers decline, or wish to decline, the installation of a smart meter in whole or in part to protect their privacy. In response, some state public utility commissions have adopted "opt-out" policies that allow customers to decline the installation (or operation) of smart meter devices. For example, in March 2012, the Public Utility Commission of Nevada approved an

---

230. This central regulatory role for public utility commissions may, itself, shape the deployment and regulation of smart grid technology so as to reduce the generation, availability, and usefulness of electricity use data. *See* Quinn & Reed, *supra* note 16, at 862–91 (demonstrating how utility control of smart meter information, privacy concerns, and other decisions about the architecture of the smart grid may frustrate innovation and prevent the emergence of an interstate data market).

231. *See infra* Part III.B.1 (describing opt-out policies).

232. *See infra* notes 240-265 and accompanying text (describing the privacy policy adopted by the Colorado Public Utility Commission); *see also* CAL. PUB. UTILS. COMM'N, DECISION NO. 11-07-056, DECISION ADOPTING RULES TO PROTECT THE PRIVACY AND SECURITY OF THE ELECTRICITY USAGE DATA OF THE CUSTOMERS OF PACIFIC GAS AND ELECTRIC COMPANY, SOUTHERN CALIFORNIA EDISON COMPANY, AND SAN DIEGO GAS & ELECTRIC COMPANY 2–5 (2011), *available at* http://docs.cpuc.ca.gov/WORD_PDF/FINAL_DECISION/140369.pdf (adopting privacy rules applicable to certain California utilities).

233. As noted above, privacy policies can directly impose limits on government access or, by failing to impose adequate limits, invite backlash that will ultimately result in such limits. *Supra* note 229 and accompanying text.

234. Some California cities, for example, imposed moratoria on the installation of smart meters motivated in part by privacy concerns. *Clearlake Bans PG&E Smart Meters, Utility Unfazed*, SMARTGRID TODAY (Apr. 1, 2011), http://www.smartgridtoday.com/public/Clearlake_bans_PG.cfm (describing a moratorium adopted by the city of Clearlake, California).

opt-out plan that will allow objecting customers to decline smart meter installation in favor of a digital meter that allows for drive-by reading.[235] California's Public Utility Commission has approved opt-out plans allowing customers to choose analog meters.[236] Utility commissions in other states have likewise adopted or are considering adopting similar opt-out policies.[237] Customer refusal of smart meter devices may impede the collection of personal environmental information and associated efforts to regulate environmentally significant individual behaviors directly by hindering the deployment and use of smart meter technology and by preventing installation of the technology at specific residences, and indirectly by raising the costs of smart meter deployment.[238]

2. Privacy Policies

Privacy policies adopted by state public utility commissions may impede the use of smart meter data to regulate environmentally significant individual behaviors by hindering the development and use of home energy management systems or defining the terms of

---

235. PUB. UTIL. COMM'N OF NEV., DOCKET NO. 11-10007, INVESTIGATION REGARDING NV ENERGY'S ADVANCED SERVICE DELIVERY METER PROGRAM A/K/A SMART METER AND ITS IMPLEMENTATION (2012) [hereinafter NEVADA OPT-OUT ORDER].

236. CAL. PUB. UTIL. COMM'N, DECISION MODIFYING PACIFIC GAS AND ELECTRIC COMPANY'S SMARTMETER PROGRAM TO INCLUDE AN OPT-OUT OPTION, DECISION NO. 12-02-014 (2012), *available at* http://docs.cpuc.ca.gov/PUBLISHED/FINAL_DECISION/159342.htm. The California Public Utilities Commission has also approved opt-out analog options for the customers of Southern California Edison and San Diego Gas & Electric. Press Release, Cal. Pub. Util. Comm'n, CPUC Approves Analog Meter Options for Edison and SDG&E Customers Who Do Not Wish to Have a Wireless Smart Meter (Apr. 19, 2012) (on file with author).

237. ME. PUB. UTIL. COMM'N, ORDER (PART I) (2011) (requiring that utility customers in Maine be given the option to retain analog meters or use smart meters with the transmission function disabled); MD. PUB. SERV. COMM'N, NOTICE OF HEARING AND OPPORTUNITY TO COMMENT ON AN "OPT-OUT" OPTION FOR SMART METERS (2012) (scheduling a "legislative-style hearing . . . to address whether to require the subject utilities to offer customers an opportunity to opt out of receiving a smart meter should they so choose").

238. The costs of providing alternate metering services to customers who opt out can be high and can include "installation labor, meter testing labor, customer support and application processing labor, ancillary meter supplies, customer communications materials, . . . returning [the utility's] system to its standard configuration, . . . system modification expenditures, handheld purchasing costs, meter reading costs, back-office labor costs, materials costs, and annual hardware and software maintenance costs." NEVADA OPT-OUT ORDER, *supra* note 235, at 21. Notably, however, opt-out policies often allow utilities to charge customers who opt out for the additional costs of nonstandard service. *Id.* at 29 ("[T]he cost of the trial opt-out tariff must be borne by the customers who demand, for whatever reason, the tariff that results in incremental costs to [the utility].").

government agency access to smart meter data.[239] Utility commission privacy policies vary and are being updated in many states to accommodate advanced meter deployment.[240] Colorado's policy provides a useful example.[241]

In Colorado, customer consent has long been required for the disclosure of personal information[242] by utilities,[243] although there are exceptions. Utilities in Colorado are permitted to provide personal information to requesting government agencies without consent.[244] The definition of personal information is broad, and it is not clear

---

239. Of note, as discussed *infra* note 277 (discussing the potential application of the Stored Communication Act to utilities), federal statutory privacy protections may apply to and impose independent constraints on the disclosure of smart meter information.

240. In Texas, for example, electric service providers are prohibited from releasing "proprietary customer information," except in certain enumerated circumstances—which notably do not include releasing such information to local, state, or federal agencies, except for law enforcement agencies, consumer reporting agencies, and energy assistance agencies. 16 TEX. ADMIN. CODE § 25.472(b) (2012). Propriety customer information means:

> Any information compiled by an electric utility on a customer in the normal course of providing electric service that makes possible the identification of any individual customer by matching such information with the customer's name, address, account number, type or classification of service, historical electricity usage, expected patterns of use, types of facilities used in providing service, individual contract terms and conditions, price, current charges, billing records, or any other information that the customer has expressly requested not be disclosed. Information that is redacted or organized in such a way as to make it impossible to identify the customer to whom the information relates does not constitute proprietary customer information.

Id. § 25.272(c)(5).

241. California has also adopted a smart grid privacy policy. CAL. PUB. UTIL. COMM'N, DECISION ADOPTING RULES TO PROTECT THE PRIVACY AND SECURITY OF THE ELECTRICITY USAGE DATA OF THE CUSTOMERS OF PACIFIC GAS AND ELECTRIC COMPANY, SOUTHERN CALIFORNIA EDISON COMPANY, AND SAN DIEGO GAS & ELECTRIC COMPANY, DECISION NO. 11-07-056 app. D (2011) [hereinafter CPUC PRIVACY POLICY], *available at* http://docs.cpuc.ca.gov/published/FINAL_DECISION/140369.htm. The California Public Utilities Commission's privacy policy implements state law. CAL. PUB. UTIL. § 8380 (West 2012) (setting forth statutory privacy protections for energy consumption data).

242. Colorado regulations define "personal information" as follows:

> 'Personal information' means any individually identifiable information obtained by a regulated entity from a customer, from which judgments can be made regarding the customer's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics. Personal information does not include: a customer's telephone number if it is published in a current telephone directory or is scheduled to be published in the next telephone directory; information necessary for the billing and collection of amounts owed to a public utility or to a provider of service using the facilities of a public utility; or Standard Industrial Code information used for purposes of directory publishing.

4 COLO. CODE REGS. § 723-1:1004(u) (LexisNexis 2010).

243. *Id.* § 723-1:1104(a).

244. *Id.* § 723-1:1104(d) ("A utility may disclose personal information requested by a federal, state, or local governmental agency including, but not limited to: the Commission; state and local departments of social services; and federal, state, and local law enforcement agencies.").

whether smart meter data constitute personal information; however, the regulations expressly provide that "information necessary for the billing and collection of amounts owed to a public utility or to a provider of service using the facilities of a public utility" is not considered personal information.[245] Thus, if smart meters were used to track energy use at frequencies required to impose time-of-use or critical-load pricing, detailed information about household energy use would be "necessary for billing" and therefore would not be personal information.[246]

New data privacy rules that regulate Colorado electric utilities and were designed specifically to address privacy issues raised by smart meter deployment went into effect in February of 2012.[247] The new rules establish an opt-in procedure; although subject to some exceptions, utilities are generally prohibited from releasing customer data unless the customer has authorized the release of the data by submitting a consent form.[248] Utilities are authorized to "use customer data to provide regulated utility service in the ordinary course of business"[249] and to share customer data with "contracted agents," provided they contract with those agents for certain privacy protections (contracted agents may only, for example, use the information for the purposes specified in the contract and not for any secondary commercial purpose).[250] Utilities are also authorized to release aggregated data reports[251] subject to some restrictions designed to avoid reverse engineering that would allow isolation of one customer's data from the aggregated data pool.[252]

Colorado's data privacy rules thus impose some constraints on private, third party deployment of products to help individuals understand and manage their home energy use using smart meter data. With respect to private vendors, Colorado's privacy protections impose a specific procedure—customers must complete and submit a consent form.[253] Although not perhaps unduly burdensome, this nonetheless presents an additional barrier to the development of

245. *Id.*

246. QUINN, *supra* note 18.

247. 4 COLO. CODE REGS. § 723-3:3026–31.

248. *Id.* §§ 723-3:3026, 3028, 3030.

249. *Id.* § 723-3:3026(a).

250. *Id.* § 723-3:3029.

251. *Id.* § 723-3:3031.

252. PUB. UTIL. COMM'N OF COLO., IN RE PROPOSED RULES RELATING TO SMART GRID DATA PRIVACY FOR ELECTRIC UTILITIES, DECISION NO. R11-0922 ¶ 88 (2011), *available at* https://www.dora.state.co.us/pls/efi/efi_p2_v2_demo.show_document?p_dms_document_id=128569.

253. 4 COLO. CODE REGS. §§ 723-3:3028, 3030.

technologies to support voluntary conservation behavior.[254] With respect to vendors that a utility contracts with directly, Colorado's rule would treat the company as a contracted agent and require that the utility's contract with the company include certain privacy protections.[255]

The terms of government access to household energy use data under the data privacy rules are somewhat unclear. The data privacy rules, set forth in the Rules Regulating Electric Utilities, provide that: "A utility shall not disclose customer data unless such disclosure conforms to these rules, except as required by law or to comply with the Commission rule. Illustratively, this includes responses to requests of the Commission, warrants, subpoenas, court orders, or as authorized by § 16-15.5-102, C.R.S."[256]

The prior rule authorizing the release of personal information to government agencies upon request, located in the Rules of Practice and Procedure, has not been amended. Thus, the question is how that rule and the new data privacy rules are meant to be interpreted together.[257] The authorization of the release of personal information upon request to government agencies is a "Commission rule" for purposes of section 3026(b), and the release of personal information absent consent is thus presumably still allowed.[258] Thus, if smart meter data is "personal information," it is likely still permissible for utilities to provide that information to government agencies upon request absent customer consent; if smart meter data is not "personal

254. *Energy Lawyer Asks: Can a Data-use Consent Form Be Too Clear?*, SMARTGRIDTODAY (May 18, 2011), http://www.smartgridtoday.com/members/Energy_lawyer_asks_Can_a_datauseltbrgt_consent_form_be_too_clear.cfm (describing concerns that Colorado's consent form will dissuade consumers from using home energy management systems).

255. 4 COLO. CODE REGS. § 723-3:3029.

256. *Id.* § 723-3:3026(b).

257. The definition of "personal information" is provided in full. *See supra* note 242. The regulations also define "customer data":

> 'Customer data' means customer-specific data or information that: (1) is collected from the electric meter by the utility and stored in its systems (e.g., kWh, kW, voltage, VARs and power factor); (2) is received by the utility from the customer identifying whether they participate in regulated utility programs, such as renewable energy, demand-side management, load management, and energy efficiency; and (3) information other than personal information that is shown on bills issued to customers for metered service furnished.

4 COLO. CODE REGS. § 723-3:3001(j). Roughly speaking, personal information appears to be meant to refer primarily to address and similar information and customer data to energy use, although the definitions are somewhat unclear.

258. An explanation provided in the decision adopting the final data privacy rules would seem to support this interpretation. PUB. UTIL. COMM'N OF COLO., *supra* note 252, ¶ 48 (resolving a similar potential conflict by observing that the authority to disclose personal information under Rule 1104 is a Commission rule that authorizes the release of customer data under rule 3026(b)).

information" and only "customer data," then disclosure would be prohibited absent consent or a subpoena.[259] It seems likely, however, that whatever the correct interpretation of these terms, the intent in drafting the data privacy rules was not to allow unfettered access by government agencies to smart meter data.[260] Thus, Colorado's new data privacy rules likely require an environmental agency seeking to access customer-specific smart meter data to obtain a subpoena or consent. Notably, as in Colorado, in California, government can obtain access to smart meter data with a subpoena or by obtaining customer consent. Additionally, however, a governmental entity can, under the supervision of the California Public Utilities Commission ("CPUC") and provided that it complies with the CPUC's privacy rules, obtain smart meter data without consent to perform "energy efficiency or energy efficiency evaluation services."[261]

As described above, the adaptation of smart meter technology to accommodate privacy concerns has largely preserved individual access to energy use data, which is widely recognized as a core benefit of smart meter deployment. However, the ramifications of these privacy policies for future uses of the smart grid remain to be seen. By imposing these privacy restrictions as the architecture of the smart grid and associated services are still being developed, utility commissions are allowing privacy concerns to shape smart grid functions:

> Interestingly, privacy concerns in Colorado seem to have struck a nerve with regulators that emissions reduction, utility profitability, and edge service market development have not. As a result, many of the decisions that affect the latter issues may be determined, for better or worse, with privacy as the dominant framework for discussion. Indeed, the usage restrictions placed on data streams in the name of privacy protection could have profound effects on competing business models' ability to leverage the value of smart grid data.[262]

---

259. 4 COLO. CODE REGS. § 723-3:3026(b).

260. PUB. UTIL. COMM'N OF COLO., *supra* note 252, ¶ 46 (expressing "sympathy to the concern" that allowing the release of customer data in response to attorney-issued subpoenas could result in "fishing expeditions for customer data," but finding "no basis or authority . . . for the Commission to limit or modify obligations arising from a legally valid subpoena").

261. CPUC PRIVACY POLICY, *supra* note 241, app. D at 7 (providing that utilities may disclose smart meter data absent consent to "a governmental entity . . . [that] provid[es] energy efficiency or energy efficiency evaluation services pursuant to an order or resolution of the Commission"); *see also id.* at 2 (defining, as a "primary purpose" "for the collection, storage, use[,] or disclosure of covered information[,]" is to "plan, implement, or evaluate demand response, energy management, or energy efficiency programs under contract with an electrical corporation, under contract with the Commission, or as part of a Commission authorized program conducted by a governmental entity under the supervision of the Commission").

262. Quinn & Reed, *supra* note 16, at 879–80 (citation omitted); *see also id.* at 862–91.

With respect to the potential regulatory value and privacy harms of providing government access to smart meter data, utility commissions seem less focused on this issue. By requiring a subpoena or consent, Colorado effectively precludes government access for some, perhaps many, regulatory purposes;[263] in California, the terms of government access are largely left to the discretion of the CPUC, which can approve government access without consent to promote energy efficiency on terms it sees fit. Colorado's approach may inadvertently frustrate government access; the impacts of California's approach will depend upon how the CPUC exercises its authority to permit government access absent consent.

C. Fourth Amendment

A desire to protect privacy in the face of new, technologically enhanced information-gathering capabilities may be influencing the development of Fourth Amendment doctrine so as to inhibit government access to information generated using those technologies. Specifically, concerns about privacy appear to be causing courts to question the meaning and scope of the third party doctrine;[264] limitations on the third party doctrine could significantly increase the administrative burdens of using technology to help detect, implement, or enforce the regulation of some environmentally significant individual behaviors.

---

263. It is questionable whether the EPA or other relevant agencies possess the statutory authority to subpoena smart meter records to promote energy efficiency programs; a consent requirement presents administrative burdens and creates the risk of selection bias. Of note, as discussed *infra* note 277 and accompanying text, apart from utility policies, government access to smart meter data may be limited by independent statutory or constitutional constraints.

264. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." (citations omitted)); United States v. Warshak, 631 F.3d 266, 282–88 (6th Cir. 2010) (holding warrant required to obtain the content of emails stored at third-party Internet Service Provider ("ISP")); Regberg v. Paulk, 611 F.3d 828, 842–46 (11th Cir. 2010) (reviewing the caselaw and concluding that the questions involved in discerning whether the Fourth Amendment applies when government obtains the content of emails from a third-party ISP are "complex, difficult, and 'far-reaching' legal issues"); *see also* CRS SMART METER PRIVACY REPORT, *supra* note 228, at 16 (discussing the reasonable expectation of privacy in smart meter data and identifying three rationales that "might weigh against the application of traditional third-party analysis" to smart meters: "(a) a person's expectation of privacy while at home; (b) the breadth and granularity of private information conveyed by smart meters; (c) the lack of a voluntary assumption of the risk or consent to release of this data"); Strandburg, *supra* note 32, at 642 ("Apparently aware of the sweeping implications of a blunderbuss approach to surveillance of digital intermediary records, these courts are increasingly disinclined to take a simplistic and aggressive third party doctrine approach.").

Fourth Amendment protections can apply to searches conducted in support of noncriminal administrative regulations.[265] The inspection of a home to enforce a municipal housing code, while an "administrative search," nonetheless requires a warrant, although in some circumstances the showing required to obtain a warrant for such a regulatory inspection is relaxed.[266] Instead of being required to establish probable cause to believe that there is a violation of the code at a particular home, the government can obtain a warrant without any "specific knowledge of the condition of the particular dwelling" upon establishing that "reasonable legislative or administrative standards for conducting an area inspection are satisfied with respect to a particular dwelling."[267] Factors relevant to deciding whether this relaxed standard governs the issuance of a warrant include the importance of the government interest at stake (the need for the inspection), whether there is a "long history of judicial and public acceptance" of the type of inspection at issue, whether the regulation at issue could feasibly be enforced without area inspections, and the extent to which the inspection invades privacy.[268]

Some types of information gathering to support the regulation of environmentally significant individual behaviors might thus, if conducted by the government, require a warrant (although perhaps obtainable upon a relaxed showing). The need to satisfy even a weakened warrant requirement would pose an administrative burden; in the context of regulating individuals, this burden could prove so

265. See v. Seattle, 387 U.S. 541 (1967); Camara v. Mun. Court of S.F., 387 U.S. 523 (1967) (rejecting warrantless administrative searches); Inc. Village of Laurel Hollow v. Laverne, Inc., 262 N.Y.S.2d 622 (N.Y. App. Div. 1965); *see also* Laura J. Kerrigan et al., *Project: The Decriminalization of Administrative Law Penalties, Civil Remedies, Alternatives, Policy, and Constitutional Implications*, 45 ADMIN. L. REV. 367, 397–98 (1993) ("The right to be free from unreasonable searches and seizures under the Fourth Amendment applies to noncriminal regulatory or administrative searches, as well as traditional criminal searches." (citations omitted)).

266. *Camara*, 387 U.S. at 534–38.

267. *Id.* at 538. William J. Stuntz has argued persuasively that many exceptions to or relaxations of Fourth Amendment protections arise from the difficulty of valuing privacy in an evenhanded way without rendering "a great deal of ordinary government activity . . . subject to searching judicial review" or "drastically reduc[ing]" "privacy-based restrictions on police searches." Stuntz, *supra* note 194, at 1055. He explains many exceptions to the Fourth Amendment as efforts by courts to permit relatively unimpeded information gathering necessary for the functioning of the modern administrative/regulatory state. *Id.* at 1054–60.

268. *Camara*, 387 U.S. at 534–39 (observing that there is a "relatively limited invasion of the urban citizen's privacy" where "inspections are neither personal in nature nor aimed at the discovery of evidence of crime").

great as to undermine the regulation's utility.[269] However, the government might obtain, by request or subpoena,[270] information from a third party who obtained that information from the individual. Under those circumstances, it is likely that the government would not need to obtain a warrant under the third party doctrine.[271] The doctrine is generally understood to provide that once an individual shares information with a third party or exposes it to the public, he or she no longer has an expectation of privacy subject to Fourth Amendment protection with respect to that information.[272]

Imagine, for example, that a city wished to access smart meter data to detect violations of a water conservation ordinance that restricted lawn watering to specified days, times, or durations.[273] Some appliances use electricity in recognizable patterns (a signature) that are discernible from the records generated by smart meters.[274]

---

269. *See generally* Stuntz, *supra* note 194, at 1032 (arguing that many types of regulation would be "impossible without compelled 'suspicionless' disclosure—disclosure that precedes any showing that the government has a strong interest in obtaining the information in this case").

270. For an overview of the use of subpoenas to obtain personal information held by third parties, see Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 822–26 (2005).

271. Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (allowing the government to install a pen register at the telephone company to record the numbers dialed from an individual's home without a warrant); United States v. Miller, 425 U.S. 435, 442 (1976) (holding that the government did not need a warrant to obtain an individual's financial records from the bank since the records contained information "voluntarily conveyed" to the bank); United States v. Hamilton, 434 F. Supp. 2d 974, 979 (D. Or. 2006) (declining to suppress utility records released in response to an administrative subpoena because the utility was a "third party recipient[ ] of information" so that the government "did not need a warrant supported by probable cause to acquire Mr. Hamilton's . . . power records"); *see also* Balough, *supra* note 2, at 184–85 (discussing the application of the third party doctrine to allow warrantless access to traditional utility records); Solove, *Digital Dossiers*, *supra* note 20, at 1133–38 (explaining how the third party doctrine frequently allows warrantless access to digital information). Of note, the Supreme Court has not ruled on the applicability of the third party doctrine with respect to digital communication, and commentators debate the scope of the doctrine. *See, e.g.*, Strandburg, *supra* note 32, at 633–49 (critiquing what she terms the "aggressive version of the third party doctrine").

272. *E.g.*, Solove, *Digital Dossiers*, *supra* note 20, at 1133–38 ("The Court's new conception of privacy is one of total secrecy. If any information is exposed to the public or if law enforcement officials can view something from any public vantage point, then the Court has refused to recognize a reasonable expectation of privacy. . . . [The Court has further held] that there is no reasonable expectation in privacy for information known or exposed to third parties.").

273. Such water conservation ordinances are common, *see, e.g.*, EL PASO, TEX., CODE § 15.13.020 (2011) (limiting lawn watering to specified dates and times), and are likely to become more common as an adaptive response to climate change–occasioned water shortages, Benjamin Houston & Noah Hall, *Managing Demand for Water*, *in* THE LAW OF ADAPTATION TO CLIMATE CHANGE (Michael Gerrard & Katrina Fischer Kuh eds., 2012) (surveying adaptation strategies for responding to reduced water availability, including residential water conservation measures).

274. *See* QUINN, *supra* note 18, at A-5:

From an examination of smart meter records, it might be possible to identify the energy use signature of automatic lawn sprinklers (a capability that if not presently available is at least reasonably foreseeable).[275] The city might ask for access to a utility's smart meter records and use software to detect repeated occurrences of the lawn sprinkler signature at forbidden times or durations at the same address (perhaps signaling that a household has automatic sprinklers that are set in a manner contrary to the water conservation ordinance). Armed with a computer-generated list of addresses, the city could then enforce the ordinance expending far fewer resources than might otherwise be required. Under the third party doctrine, households likely do not have a reasonable expectation of privacy in energy use data provided to the utility;[276] thus, the government would likely not be required to obtain a warrant.[277]

> A remarkable number of electric appliances can be identified by their load signatures, and with impressive accuracy. Researchers have all but mastered identification of the larger common household appliances such as water heaters, well pumps, furnace blowers, refrigerators, and air conditioners, with recognition accuracies approaching perfection. Ongoing work focuses now on the myriad [of] smaller electric devices around the home such as personal computers, laser printers, and differentiating fluorescent from energy-saving light bulbs.

(citations omitted); *id. at* A-8 (describing a study where researchers were able to identify the use of specific appliances from aggregated load information and observing that "[a]s libraries of load signatures expand and more research pours into similar efforts, the details extractable from smart meter data will become richer").

275. Because smart meters typically track energy consumption in intervals at or below fifteen minutes (as opposed to monthly readings), the information collected may allow a highly granular depiction of intrahome activities, especially when cross-referenced with other publicly available information. *See* NAT'L INST. OF STANDARDS & TECH., *supra* note 220, at 13.

276. *See supra* note 271 and accompanying text. Additionally, it could be argued that, third party doctrine aside, homeowners do not have a reasonable expectation of privacy with respect to when they water their lawns. *See* California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (holding that despite steps taken to prevent discovery of marijuana plot within the curtilage of suspect's home, what a person knowingly exposes to the public, even when in the home, is devoid of Fourth Amendment protection); Oliver v. United States, 466 U.S. 170, 176 (1984) (limiting the scope of a Fourth Amendment search to the interior of the home, thereby allowing conviction for an illegal grow operation discovered by police in the rear of suspect's home under the "open fields" doctrine); *cf.* Dow Chem. Co. v. United States, 476 U.S. 227, 236–39 (1986) (holding that aerial photographic discovery of CAA violations do not implicate a Fourth Amendment search absent the use of technologies that can penetrate exterior walls). But access to smart meter data would include information about a variety of other in-home activities (when the dishwasher is run, etc.) where the claim for an expectation of privacy is clearer. For analyses of whether the government is required to obtain a warrant under the Fourth Amendment to obtain smart meter records from a utility, see CRS SMART METER PRIVACY REPORT, *supra* note 228, at 7–22; Balough, *supra* note 2, at 183–85; Lerner & Mulligan, *supra* note 18, at 11–25; McNeil, *supra* note 18, at 211–18 (arguing that the third party doctrine should be interpreted so as to prohibit warrantless government access to smart meter data).

277. Of note, if by virtue of operating smart meter technology, the utility was considered a provider of electronic communication service or a provider of remote computing service and other

As various technologies cause individuals to generate and share information with third parties, the third party doctrine may permit warrantless access to increasing volumes of personal information. For this and other reasons, many privacy and technology scholars criticize the third party doctrine.[278] Some appellate courts have declined to apply the third party doctrine with respect to the content of digital communication.[279] Most notably, in her concurrence in *United States v. Jones*, Justice Sotomayor suggests that in light of technological advance, it may be necessary to "cease[ ] to treat secrecy as a prerequisite for privacy":

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[280]

---

prerequisites for application of the Stored Communications Act ("SCA") were satisfied, the Act could impose warrant or other requirements for access to or the disclosure of smart meter data in electronic storage. 18 U.S.C.A. §§ 2701–11 (West 2012). However, application of the SCA to smart meter data and utilities is, at best, uncertain. CRS SMART METER PRIVACY REPORT, *supra* note 228, at 24–28 (examining application of the SCA to smart meter data and concluding that the application of the SCA is fact-specific and possibly does not extend to data that "has arrived at the utility and resides on its servers"); Balough, *supra* note 2, at 180 (identifying "uncertainties" that "make it impossible to determine whether the SCA offers any protection from the disclosure of intimate personal data from smart meters"). State statutes, state constitutional privacy protections, utility privacy policies, and other jurisdiction-specific measures might also impose conditions on access to utility records. *See, e.g.*, IDAHO CODE ANN. § 37–2741A (West 2012) (setting forth requirements for the issuance of a subpoena for the production of records of a utility). Additionally, where utility records are considered public records, a warrant would not be required to obtain those records. CRS SMART METER PRIVACY REPORT, *supra* note 228, at 11–12 ("Law enforcement might also request smart meter data under a public records theory. It is generally accepted that public records are not accorded Fourth Amendment protection. . . . Whether a person's utility records are public records differs from state to state." (citations omitted)).

278. *E.g.*, SOLOVE, *supra* note 20, at 201–02 ("[I]t is only recently that we are beginning to see the profound implications of the third party doctrine. . . . The government's harvesting of information from the extensive dossiers being assembled with modern computer technology poses one of the most significant threats to privacy of our times." (citation omitted)); Henderson, *supra* note 77, at 50–51 (setting out four factors to guide application of the Fourth Amendment to information provided to third parties); Strandburg, *supra* note 32, at 633–49 (critiquing aggressive interpretations of the third party doctrine). *But see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 573–81 (2009) (describing functional benefits of the third party doctrine).

279. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

280. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (citations omitted).

Justice Sotomayor's concurrence signals that she is open to abandoning the third party doctrine, and perhaps even the secrecy paradigm that appears to undergird it, to protect against technologically enabled revelations about previously private behaviors.

Additionally, in permitting warrantless access to traditional utility records under state law, some state courts have emphasized that the obtained electric records do not reveal information about activities within the home.[281] For example, in *State v. Kluss*, an Idaho court upheld warrantless access to an individual's utility records, reasoning:

> The power records in the case at bar reveal only the amount of power usage. The power records were maintained by WWP [the utility company] in the ordinary course of business. They do not identify any activities of Kluss. On a comparative basis they may demonstrate that the power use at the Kluss home is greater or lesser than similar houses or at similar times or that the power use has increased or decreased at different times. The information does not provide any intimate details of Kluss's life, identify his friends or political and business associates, nor does it provide or complete a "virtual current biography." The power records unlike telephone or bank records, do not reveal discrete information about Kluss's activities. High power usage may be caused by any one of numerous factors: hot tubs, arc welders, poor insulation, ceramic or pottery kilns, or indoor gardening under artificial lights.[282]

Smart meter data can, of course, generate a great deal of information about in-home activities. The greater visibility afforded to in-home behaviors by smart meter data could thus cause some state courts to revisit reliance on the third party doctrine to permit warrantless access to utility records.

Thus, it seems possible, perhaps even likely,[283] that Fourth Amendment doctrine[284] may evolve to limit the scope of the third party doctrine in part to prevent technologically enabled invasions of privacy; abolishment or weakening of the third party doctrine could constrain government access to personal environmental information generated by this technology. If the government were required to

---

281. Samson v. State, 919 P.2d 171, 172–73 (Alaska Ct. App. 1996).

282. State v. Kluss, 867 P.2d 247, 254 (Idaho Ct. App. 1993); *see also Samson*, 919 P.2d at 173 (citing State v. Kluss, 867 P.2d 247, 254 (Idaho 1993), in upholding warrantless access to traditional utility records under Alaska's constitution); People v. Dunkin, 888 P.2d 305, 308 (Colo. App. 1994) (citing the reasoning in *Kluss*, 867 P.2d at 254, in upholding warrantless access to traditional utility records under Colorado's constitution).

283. Katherine Strandburg, for example, predicts, based on "the trend of appellate court rulings, along with the Supreme Court's conspicuous failure to rely on the third party doctrine for an easy out in *Quon*," that "the Court will, at a minimum, eventually adopt a content/noncontent distinction in the context of two-party communications." Strandburg, *supra* note 32, at 643.

284. Or the interpretation of privacy rights contained in state constitutions.

obtain a warrant even under the less demanding standard sometimes applicable to administrative searches to access, for example, utility smart meter records, this could pose a significant administrative burden. As noted above, the administrative burdens of regulating millions of individuals (as opposed to the smaller number of larger, industrial sources of pollution) has long been recognized as an obstacle to regulating environmentally significant individual behaviors, in particular with respect to the enforcement of mandates on individuals.[285]

Viewed together, the emerging privacy constraints on RFID and smart meters and the threatened constriction of the third party doctrine illustrate how privacy concerns can impact the deployment of technology, including technology that can be used to generate personal environmental information in support of the regulation of environmentally significant individual behaviors.[286] However, privacy limits on the use of RFID and smart meters and doctrinal pressure on the third party doctrine do provide apt examples of how the ability of technology to generate information about individual behaviors frequently motivates calls for, and sometimes the development of, new privacy protections that can limit the availability of personal information to support regulation.

V. CONCLUSION

This Article's core claims are that: (1) technology is increasingly making information about individual environmental behaviors and associated harms more accessible; (2) better information about environmentally significant individual behaviors could meaningfully enhance fledgling efforts to regulate those behaviors; and (3) use of technologically enabled personal environmental information in support of regulation will require the resolution of myriad privacy concerns. Successful resolution of the tension between technologically enabled access to personal environmental information, regulatory uses of that information, and

285. *See supra* notes 137–44 and accompanying text (describing how technology can reduce enforcement burdens associated with applying mandates to environmentally significant individual behaviors).

286. If faced with the prospect of securing a warrant to access information, the government could explore alternatives for obtaining that information that would not require a warrant (such as seeking consent or obtaining aggregated data scrubbed of personally identifiable information). Other obstacles to the use of mandates, in chief political feasibility, constrain the possibilities for imposing mandates on environmentally significant individual behaviors, particularly those that would require the monitoring of in-home behavior. Kuh, *supra* note 9.

privacy concerns will require an understanding of the potential regulatory and environmental benefits of technologically enabled access to personal environmental information, the constraints that privacy protections can impose on regulatory efforts and environmental results, and the type and significance of potential privacy harms resulting from access to the information. This Article identifies some of the benefits of technologically enabled access to personal environmental information in the regulation of environmentally significant individual behaviors, illustrates some of the privacy concerns and constraints that can result, and urges further contemplation of how best to value and understand claimed privacy interests in personal environmental information. Engaging the tension between regulation and privacy in this context is important because where the regulatory and environmental benefits of access to personal environmental information are not recognized or understood, technology-specific privacy limits can inadvertently frustrate access to personal environmental information and may be too stringent because policymakers and the public do not weigh the countervailing interests.[287] Where the privacy harms occasioned by access to personal environmental information are not recognized or adequately understood, policymakers risk a backlash when the privacy implications of a policy become known.[288] And proceeding in the absence of a thoughtful conceptualization of the value and contours of privacy in the context of individual environmental harms presents the risk that debates about balancing privacy and policy objectives will reach undesirable outcomes that either over- or undervalue the privacy interests at stake.[289] For all of these reasons, environmental scholars and others should, in the words of Justice Breyer, join a "national conversation" about how to reach an optimal balance between access to personal environmental information and privacy.[290]

287. Overly robust privacy protections have been critiqued for giving rise to perverse results. Hirsch, *supra* note 147, at 9 n.36 (describing disputes about "the importance of privacy as a societal value").

288. *Smart Grid Elevated to Top Issue by Leading Privacy Watchdogs*, SMARTGRID TODAY (Dec. 17, 2009), http://www.smartgridtoday.com/members/1060.cfm (" '[G]et one really salient privacy invasion that makes the front page of the *New York Times* and the *Washington Post* and you'll bring to a dead stop smart grid development.' " (quoting Elias Quinn)).

289. Hirsch, *supra* note 147, at 9 n.36.

290. Breyer, *supra* note 36, at 263.

***