Self-Surveillance Privacy

Jerry Kang, Katie Shilton, Deborah Estrin, Jeff Burke, and Mark Hansen[*]

ABSTRACT: It has become cliché to observe that new information technologies endanger privacy. Typically, the threat is viewed as coming from Big Brother (the government) or Company Man (the firm). But for a nascent data practice we call "self-surveillance," the threat may actually come from ourselves. Using various existing and emerging technologies, such as GPS-enabled smartphones, we are beginning to measure ourselves in granular detail—how long we sleep, where we drive, what we breathe, what we eat, how we spend our time. And we are storing these data casually, perhaps promiscuously, somewhere in the "cloud" and giving third parties broad access. This data practice of self-surveillance will decrease information privacy in troubling ways. To counter this trend, we recommend the creation of the Privacy Data Guardian, a new profession that manages Privacy Data Vaults, which are repositories for self-surveillance data. In addition to providing technical specifications of this approach, we outline the specific legal relations, which include a fiduciary relationship, between client and Guardian. In addition, we recommend the creation of an evidentiary privilege, similar to a trade-secret privilege, that protects self-surveillance data held by a licensed Guardian. We also answer objections that our solution is implausible or useless. We conclude by

[*] Jerry Kang is Professor of Law, UCLA School of Law, Professor of Asian American Studies (by courtesy), Korea Times—*Hankook Ilbo* Chair in Korean American Studies. <kang@law.ucla.edu> <http://jerrykang.net>. Katie Shilton is Assistant Professor, College of Information Studies, University of Maryland. Deborah Estrin is UCLA Henry Samueli School of Engineering and Applied Science, Professor of Computer Science, Professor Electrical Engineering, Jon Postel Chair in Computer Networks, and Founding Director of the Center for Embedded Networked Sensing (CENS). Jeff Burke is Assistant Professor, UCLA School of Film, Theater & Television; Executive Director of REMAP, the Center for Research in Engineering, Media and Performance. Mark Hansen is Professor of Statistics, UCLA Department of Statistics; Professor (by courtesy) of Design|Media Art and Electrical Engineering.

Helpful research assistance was provided by Jonathan Feingold, Emily Reitz, and Isaac Silverman. This paper was presented at the George Washington University School of Law Faculty Colloquium 2011, Privacy Law Scholars Conference 2009, and UCLA School of Law Summer Workshop Series 2009. We are thankful for comments from Richard Abel, Ann Carlson, Eric Goldman, Dennis Heinson, Dennis Hirsch, Jeff Jonas, Sung Hui Kim, Ken Klee, William Klein, Tim Malloy, Jon Michaels, Stephen Munzer, Helen Nissenbaum, Marc Rotenberg, Noah Zatz, and Eric Zolt. This research was supported in part by the UCLA Academic Senate, UCLA School of Law, and the UCLA Center for Embedded Network Sensing.

pointing out that various legal, technological, and self-regulatory attempts at safeguarding privacy from new digital, interconnected technologies have not been particularly successful. Before self-surveillance becomes a widespread practice, some new innovation is needed. In our view, that innovation is a new "species," the Personal Data Guardian, created through a fusion of law and technology and released into the current information ecosystem.

I. INTRODUCTION

It has become cliché to observe that new information technologies endanger privacy. Typically, the threat is viewed as coming from Big Brother (the government) or Company Man (the firm). But for a nascent data practice we call "self-surveillance," the threat may actually come from ourselves. Using various existing and emerging technologies, such as GPS-enabled smartphones, we are beginning to measure ourselves in granular detail—how long we sleep, where we go, what we breathe, what we eat, how we spend our time. And we are storing these data casually, perhaps promiscuously, somewhere in the "cloud" and giving third parties broad access. This practice of self-surveillance will decrease information privacy in troubling ways. To counter this trend, we recommend the creation of the Personal Data Guardian ("PDG"), a new professional who manages Personal Data Vaults ("PDVs"), which are repositories for self-surveillance data.

In Part II, we describe the emerging data practice of self-surveillance, which has been enabled by new measurement and communication technologies. We explain how self-surveillance can produce substantial benefits to both the individual and society. Unfortunately, such benefits may never be achieved without substantial privacy costs.

Part III makes threshold clarifications about those privacy costs. It offers two different metrics by which privacy might be measured and explains why the rise of self-surveillance will cause a net loss of privacy under either metric. We also point out that the problem of self-surveillance (our surveilling of us) is, fortunately, more tractable than related privacy problems, such as third-party surveillance of us and our surveillance of third parties.

Having cleared this brush, we turn to our central proposal in Part IV—the creation of the PDG, a professional whose job is to maintain an individual client's self-surveillance data in a PDV. In addition to providing technical specifications of this approach, we outline the specific legal relations, which include a fiduciary relationship between individual client and PDG. In addition, we recommend the creation of a topical evidentiary privilege, similar to a trade-secret privilege, that protects self-surveillance data held by the PDG.

Finally, Part V answers objections that our solution is implausible or useless. We conclude by pointing out that various legal, technological, and self-regulatory attempts at safeguarding privacy from new digital, interconnected technologies have not been particularly successful. Before self-surveillance becomes a widespread practice, some new innovation is needed. In our view, that innovation is a new designer "species," the PDG, engineered through law and technology, and released into the information ecosystem.

II. SELF-SURVEILLANCE

A. *NEW MEASUREMENT TECHNOLOGIES*

Bloggers and webmasters are familiar with Google Analytics—a widely adopted set of visualization tools that support examination of website traffic patterns.[1] A script sends website-visitor data to Google, which then analyzes the traffic patterns with remarkable granularity and provides results through flexible visuals. One can easily see the IP address of who has visited, from where (geographically and from which prior page), when, how often, for how long, and through which keyword search. It's also free of charge.

What's interesting is that new technologies allow us to cull, then analyze, similar sorts of details about not only our websites but also ourselves. Here are three examples. RescueTime.com allows the installation of a small software application that tracks how we spend time on our computer, down to the second.[2] If you want to know how much time you waste surfing particular websites, on an average Monday, you can easily collect that data.

Second, GPS manufacturer Garmin's connect.garmin.com is a web application that records our location in order to analyze outdoor training and fitness regimens.[3] If you are curious about how long your typical morning jogs are, and whether you are improving your pace, it is now simple to collect that information and analyze it.

Finally, Fitbit is a tiny piece of hardware that can be clipped on your clothing and measures how many steps you have taken, how active you have generally been, and how many calories you have burned.[4] In addition, it can track your sleep, and all these data are uploaded wirelessly to their website,

[1] *See* GOOGLE ANALYTICS, http://www.google.com/analytics/ (last visited Jan. 16, 2012).

[2] As of December 2010, RescueTime advertises two products, Pulse and Empower. The Pulse product is for "employee tracking" by management; in this sense, it is old-school surveillance. By contrast, the Empower product is more for self-analytics in that an individual voluntarily initiates the data collection for self-analysis. But even in this context, the meaning of the data collected turns on "peer" comparisons. *See* RESCUETIME, http://www.rescuetime.com/ (last visited Jan. 16, 2012).

[3] *See* GARMIN CONNECT, http://connect.garmin.com (last visited Jan. 16, 2012); *see also* DAYTUM, http://daytum.com/ (last visited Jan. 16, 2012) (making use of Google charting API); ME-TRICS, http://beta.me-trics.com/ (last visited Jan. 16, 2012) (pulling data from RescueTime and Twitter and others); MYCROCOSM, http://mycro.media.mit.edu/ (last visited Jan. 16, 2012) ("[A] web service that allows you to share snippets of information from the minutiae of daily life in the form of simple statistical graphs."); NIKE+DASHBOARD, http://nikerunning.nike.com/nikeos/p/nikeplus/en_us/plus#//dashboard (last visited Jan. 16, 2012); YOUR.FLOWINGDATA, http://your.flowingdata.com/ (last visited Jan. 16, 2012) (providing wide-open flexibility over data that can be tracked).

[4] *See* David Pogue, *Getting Fit with 2 Bits of Help*, N.Y. TIMES (Dec. 17, 2009), http://www.nytimes.com/2009/12/17/technology/personaltech/17pogue.html.

which provides pretty graphs of the day and night's activity level.[5] A similar device called DirectLife, from Philips, includes data analysis and coaching from fitness and nutrition experts.[6]

B. Self-Surveillance Defined

These examples portend the rise of "self-surveillance"—a data practice that measures, collects, and stores self-surveillance data. Self-surveillance data, in turn, are measurements of the individual self,[7] initiated by the self, using sensors that are in one's control, for the primary purpose of measuring the self. By "measurements of the self," we mean a recording (fixed expression) of an observation about the self, which may include the environment to which the self is exposed. These data include metadata about the data recorded, such as the time and place of the sensing moment. By "in one's control," we mean that these devices are under a person's direct physical control, such as a heart-rate meter that stores data onto local flash memory in one's physical possession. They could also be under more indirect control, the degree to which could be measured by the ease with which the person can simply turn off data collection without large transaction costs or loss of services from third parties.[8]

Self-surveillance data include, but are not restricted to, data collected through non-subjective and automatic sensors. By "non-subjective," we mean that they record data, such as location or acceleration, without asking for subjective introspection or self-report from the individual. Also, these are "automatic" in that they collect data in a set-it-and-forget-it mode, which,

[5] *Id.*

[6] *See* PHILIPS DIRECTLIFE, http://www.directlife.philips.com/ (last visited Jan. 16, 2012).

[7] In our definition, self-surveillance data refer only to individual human beings and not to, for example, data about corporations or other fictional legal persons. For an explanation of why we exclude non-human persons, see Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1210–11 (1998).

[8] "Self-surveillance" is an odd term, and "self-monitoring" could be used in the alternative. We prefer the more jarring phrase because "surveillance" evokes greater threat, which we think is warranted given the privacy stakes. Moreover, we want to question the psychological and philosophical assumption that a person is so unified and internally consistent, especially over time, that the idea of surveilling oneself seems silly, as if we had to keep an eye on our own left hand lest it do something bizarre or inappropriate. For example, at a single moment, a person may have conflicting desires—think about wanting dessert (when we don't want to want it) or avoiding exercise (when we want to want it). In such cases, it seems reasonable to suggest that one part of the self is surveilling another part, in order to constrain or facilitate certain behaviors. The point is more vivid if we think about moments separated in time. Imagine that Johnny "consented" at the age of sixteen to disclose certain images or facts on the Internet. Now, at the age of thirty, Johnny regrets those disclosures but cannot delete the information from public view. Johnny (present) is, of course, considered to be the same person as Johnny (past). Yet it seems reasonable to suggest that Johnny (past) has bound Johnny (present) through certain information choices made previously. Put another way, Johnny (present) is subject to a sort of data surveillance inflicted upon him by Johnny (past).

after initial configuration by the individual, does not require manual input of information on an incident-by-incident basis.

Non-subjectivity and automaticity make it more likely that huge data streams will be collected invisibly in the background. That said, these features are not definitionally necessary for self-surveillance. For instance, we would count as self-surveillance the Experience Sampling Method ("ESM") developed by psychologist Mihaly Csikszentmihalyi[9]—which involves carrying a device that regularly prompts an individual for self-reports about her status, such as happiness—even though the answers rely on self-reports and not external measurements.[10] Similarly, we would count as self-surveillance a calorie-counting practice that requires the individual to photograph all food eaten, even though such data capture isn't automatic (in the sense that taking the picture requires manual actuation at meals).[11]

C. Participatory Sensing: An Example

To make our discussion more concrete, we explore a specific case study of self-surveillance—Participatory Sensing—developed at UCLA's Center for Embedded Network Sensing ("CENS").[12] Participatory Sensing coordinates mobile devices, such as smartphones, for use as self-surveillance, personal-wellness, and research instruments. To support the widest audience of users, Participatory Sensing uses off-the-shelf mobile phones[13] running specialized software.[14] The software collects data using phones' available onboard

[9] *See* MIHALY CSIKSZENTMIHALYI, FLOW: THE PSYCHOLOGY OF OPTIMAL EXPERIENCE 4 (1990).

[10] *See, e.g.*, Christie Napa Scollon et al., *Experience Sampling: Promises and Pitfalls, Strengths and Weaknesses*, 4 J. HAPPINESS STUD. 5, 5–8 (2003) (describing interval-contingent, event-contingent, and signal-contingent sampling procedures).

[11] With any definition, there will be hard cases. For example, one could analyze one's eating patterns by examining one's credit-card transactions. Should, then, using a credit card be considered "self-surveillance" and the transactions listed on a monthly credit-card bill deemed "self-surveillance data"? We think this falls outside our definition. Most importantly, the credit-card data are collected for the primary purpose of facilitating a credit transaction and accurate billing, not for measuring oneself. In addition, the credit-card-transaction network is not obviously in one's direct or indirect control.

[12] *See* URBAN SENSING, http://urban.cens.ucla.edu/ (last visited Jan. 16, 2012).

[13] Widespread penetration and use of mobile phones make them attractive tools for Participatory Sensing and other types of self-monitoring. These always on, always present devices can capture locations and context information, infer habits and routines, and provide detailed, individualized assessments of behavioral and environmental factors.

[14] Participatory Sensing is inspired by, and draws its name from, the broader tradition of *participatory research* ("PR"). PR is a set of methods that position research subjects as co-investigators. *See* Margaret Cargo & Shawna L. Mercer, *The Value and Challenges of Participatory Research: Strengthening Its Practice*, 29 ANN. REV. PUB. HEALTH 325 (2008). PR traditions develop their research questions with the cooperation of partner communities and engage community members in research design, implementation, analysis, and dissemination. Involvement with every stage of the research process allows participants to target local knowledge and benefit from the results of systematic investigations. PR successes in health and environmental research

sensors: camera, microphone, GPS or cell-tower location, accelerometers, user-prompted entry, and Bluetooth connections to other devices. The software then uploads the geo-coded and time-stamped data to a server that performs data processing, aggregation, and modeling and displays the results to each user via private web interfaces.

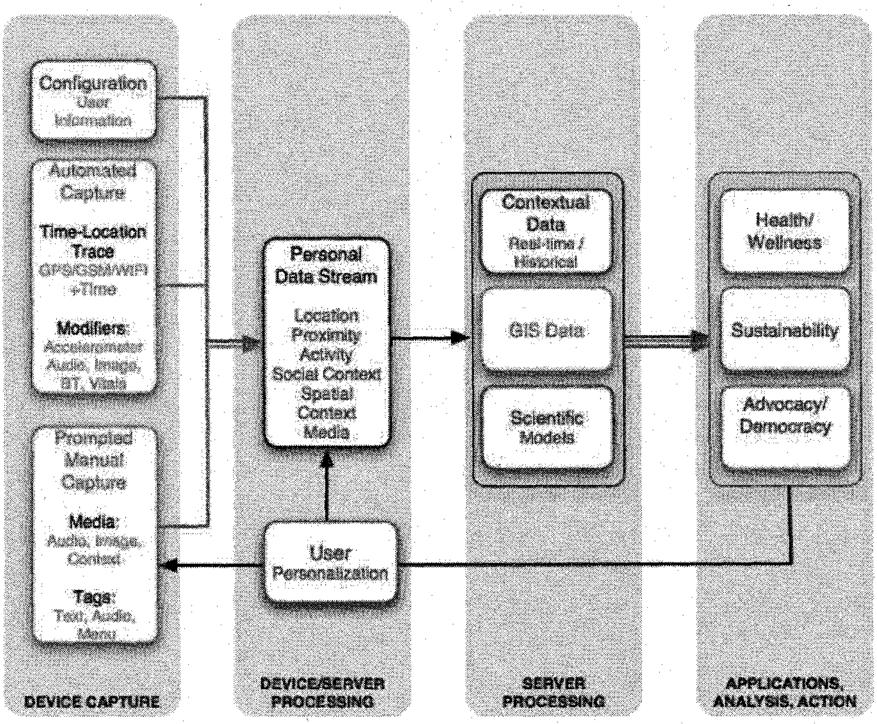

Figure 1. Participatory Sensing Processes

Participatory Sensing relies on a series of processes, as shown in Figure 1. Smartphones automatically record the time and the location of a participant by sampling GPS or cell-tower location. The "Personal Data Stream" captured by the mobile device is then automatically uploaded to secure servers via the wireless mobile-phone network. The server processes the data using models to estimate participant activities; for example, by using location and velocity, the server can determine whether the individual is walking, running, biking, or driving.

Traces that combine time, activity, and location can also support various health applications. For example, changes in work, sleep, and weekend activities can serve as indicators of fatigue, depression, or increasing side

have improved the ability of marginalized or underserved groups to act on the results of the data they have helped collect and analyze. *See, e.g.*, Carol R. Horowitz et al., *Community-Based Participatory Research from the Margin to the Mainstream: Are Researchers Prepared?*, 119 CIRCULATION 2633 (2009).

effects. Similarly, features of location-activity traces, such as how much, how quickly, and how far a person walks outdoors, can serve as outcome markers for treatment of neuromuscular diseases or rehabilitation from stroke or surgery. Specific aspects of health status, such as pain, side effects, physiological self-measurements, and medication-adherence patterns, can also be sampled using the ESM described above.[15] For example, the smartphone can prompt the user to check and enter a physiological parameter (e.g., blood glucose) or a perception such as dizziness level. The mobile phone geo-codes and timestamps these responses and uploads them to the individual's data store to create an additional time series. The server can also link the data to web-based Geographic Information Systems that, for example, document environmental hazards such as air pollution, name places and contexts (e.g., bars, home, etc.), and record characteristics of a community or social environment.

Third-party application-service providers ("3P-ASPs") can create the processing and models necessary to begin interpretation of Participatory Sensing data. For instance, CENS projects have included a wellness application that helps users discover when and where they engage in eating that is "off plan" or different from their objectives; a health application that helps chronic-illness sufferers track relationships between medicine adherence, side effects, and personal mobility;[16] a project for biking commuters to collect and compare their cycling routes; and the Personal Environmental Impact Report ("PEIR")— an application that gives users daily feedback on both their carbon footprint and their exposure to air pollution.[17] Participants can use these models as jumping off points for their own interpretations, or, in even more participatory projects, collaborate with application providers on new model creation.

[15] *See generally* CSIKSZENTMIHALYI, *supra* note 9 (discussing how certain externalities affect perceptions of live experiences).

[16] *See* Deborah Estrin & Ida Sim, *Open mHealth Architecture: An Engine for Health Care Innovation*, 330 SCIENCE 759 (2010); John Hicks et al., *AndWellness: An Open Mobile System for Activity and Experience Sampling*, WIRELESS HEALTH, Oct. 5–7, 2010, at 34.

[17] *See Our Projects*, URBAN SENSING, http://urban.cens.ucla.edu/projects/ (last visited Jan. 16, 2012). Although we have highlighted self-surveillance examples, other CENS Participatory Sensing projects extend far beyond this scope. Indeed, such research was launched initially to support sensing activities in which people decide what, how, and when to sense not only themselves but features of the world around them to collect and analyze geo-tagged imagery in support of ecological, public health, and cultural goals. For example, data can be collected as part of an explicit campaign undertaken by many users in collaboration. One such campaign focused on recycling practices on the UCLA campus. Project participants used phone cameras to document and tag incidences of recyclable materials thrown into garbage cans on campus. The incidents were tallied, mapped, and reported to campus facilities to suggest the most urgent places to add new recycling bins. *See Garbage Watch*, URBAN SENSING, http://urban.cens.ucla.edu/projects/gabagewatch/ (last visited Jan. 16, 2012). The point here is to make clear that CENS Participatory Sensing projects can easily extend beyond self-surveillance.

D. BENEFITS OF SELF-SURVEILLANCE

People engage in self-surveillance out of a natural interest in themselves. Once collected, personal data can be processed to produce self-knowledge[18] that has instrumental and intrinsic value, not only to individuals but also to society.

1. Individual Benefits

From an instrumental perspective, these techniques can improve an individual's efficiency. For example, by collecting data about how we spend our time, we can spot trends, patterns, and interdependencies that allow us to use this scarce resource more productively. In addition to decreasing waste, we can also reach our goals more effectively. As the saying goes, "What gets measured gets done."[19] For example, if the goal is to watch what we eat, a systematic record of our eating behavior as compared to casual memory can provide a more accurate caloric and nutritional breakdown of the food we consume. As another example, if we are concerned about the carbon footprint we impose on the environment, self-surveillance of our energy consumption can tell us what kind of emissions we should account for.

There may also be less instrumental and more intrinsic values for the individual. For example, we may have deeply inaccurate (and often self-serving) portraits of ourselves. Self-surveillance may demonstrate, for instance, that we navigate a far less ethnically diverse neighborhood than we suppose; that we waste more energy than our hybrid bumper stickers signal; that we yell at our children embarrassingly often; and that we have implicit biases that we explicitly reject.[20] Precise, data-driven self-measurements, alloyed with legible interfaces (with telling visuals), can provide more accurate, or at least novel, self-understanding.

Benjamin Franklin pursued this sort of self-surveillance to inculcate personal virtue, albeit using low-tech tools.[21] For most of his life, Franklin carried with him a little "account book" recording his daily performance on thirteen separate virtues. When Franklin was eighty years old, Pierre Jean Georges Cabanis saw the book and remarked:

[18] We want to highlight that self-surveillance data are rarely used only in isolation. More complete self-knowledge often requires analysis that examines trends and makes comparisons with reference populations, or "peers."

[19] This quotation is attributed to organizational theorist Mason Haire by THOMAS J. PETERS & ROBERT H. WATERMAN, JR., IN SEARCH OF EXCELLENCE: LESSONS FROM AMERICA'S BEST-RUN COMPANIES 268 (1982).

[20] *See, e.g.*, PROJECT IMPLICIT, http://projectimplicit.org (last visited Jan. 16, 2012) (providing an online example of tests used to measure automatic associations). For recent discussion of implicit bias in the law reviews, see Jerry Kang & Kristin Lane, *Seeing Through Colorblindness: Implicit Bias and the Law*, 58 UCLA L. REV. 465 (2010).

[21] Franklin never completed writing his planned work THE ART OF VIRTUE, but he referred to his practice in his autobiography. *See* Norman S. Fiering, *Benjamin Franklin and the Way to Virtue*, 30 AM. Q. 199, 200 (1978).

> We have had in our hands this precious little book. One perceives in it a sort of chronological history of Franklin's mind and character. One sees him develop, fortify and mold all the actions which constitute spiritual perfection, and the art of life and virtue taught in the same manner as that of playing an instrument or manufacturing weapons.[22]

In Franklin's own words: "I was supriz'd [sic] to find myself so much fuller of Faults than I had imagined, but I had the Satisfaction of seeing them diminish."[23] He also wrote: "[O]n the whole, tho' I never arrived at the Perfection I had been so ambitious of obtaining, but fell far short of it, yet I was by the Endeavour a better and a happier Man than I otherwise should have been if I had not attempted it."[24]

Few have the self-discipline reflected in Franklin's subjective, manual recording habits. But new technologies such as Participatory Sensing can automate much of the recording process.

2. Societal Benefits

The data collected from self-surveillance can also benefit society. Again, from an instrumental perspective, it is not only the self-interested individual who seeks to better herself. A well-functioning society seeks similar ends via "evidence-based" practices. This is why CENS has encountered immense interest from the fields of public health, epidemiology, urban planning, and resource monitoring. For instance, as a matter of fighting childhood obesity, it may be crucial to get accurate data about physical activity, food consumption, and exposure to "fast-food" advertisements and chains. Mobile Participatory Sensing data can supplement, improve, or replace current self-reports based on faulty memory that provide poor-quality data. Improved data could produce better diagnoses and more effective interventions.

From a less instrumental perspective, we recognize that collecting data about ourselves and sharing them with our neighborhoods, groups, and communities can promote a deeper collective self-understanding, not only of the present but also as it relates to the past.[25] Indeed, data can become a

[22] *Id.* at 215–16 (quoting Pierre Cabanis's statement in ALFRED OWEN ALDRIDGE, FRANKLIN AND HIS FRENCH CONTEMPORARIES 206 (1957)).

[23] BENJAMIN FRANKLIN, THE AUTOBIOGRAPHY OF BENJAMIN FRANKLIN 155 (Leonard W. Labaree et al. eds., 2d ed. 1964).

[24] *Id.* at 156.

[25] *See generally* Jerry Kang & Dana Cuff, *Pervasive Computing: Embedding the Public Sphere*, 62 WASH. & LEE L. REV. 93 (2005) (including commentary on transparency discussion). Consider, for example, not Google Analytics but Google Trends, which provides visualizations of the relative frequencies of certain search terms. *See* GOOGLE TRENDS, http://www.google.com/trends (last visited Jan. 16, 2012).

sort of currency with which we can participate in and help construct communities of memory.[26]

Notwithstanding all these substantial individual and societal benefits, some people may choose not to engage in self-surveillance because of privacy fears. Fears that such telling data might fall into the wrong hands,[27] be used in unsavory ways, or come back to harm the individual can discourage individuals from collecting the data in the first place. We must therefore confront the oxymoronic problem of self-surveillance privacy.[28]

III. THRESHOLD CLARIFICATIONS

A. *PLAUSIBLE PRIVACY METRICS*

Whenever we confront new information technologies and practices, it's easy to raise privacy fears with vaguely Orwellian and Luddite overtones. But a systematic analysis requires, first, some attempt at definitions. What is "privacy," and how might we measure it?

1. A Standard Metric: Control

The legal and policy literature typically defines information privacy as the degree to which an individual can control the collection, disclosure, and use of personal data.[29] In other words, privacy is a measure of an individual's power over the processing of information about herself. This is a *control* conception of privacy: The more control (of personal data), the more privacy.[30]

[26] *Cf.* Arjun Appadurai, *Archive and Aspiration*, *in* INFORMATION IS ALIVE: ART AND THEORY ON ARCHIVING AND RETRIEVING DATA 14, 17 (2003); Sue McKemmish, *Evidence of Me* . . . , 24 ARCHIVES & MANUSCRIPTS 28 (1996).

[27] In addition to hackers, one could worry about underpoliced employees with access to servers. *See, e.g.*, Phil Wong, *Conversations About the Internet #5: Anonymous Facebook Employee*, RUMPUS (Jan. 11, 2010), http://therumpus.net/2010/01/conversations-about-the-internet-5-anonymous-facebook-employee/ (explaining how employees casually viewed private user profiles with a master word that was a variant of "Chuck Norris" (internal quotation marks omitted)).

[28] For a discussion of why we chose this term, see *supra* note 8.

[29] Sometimes, privacy is phrased not as a measure of capacity but as a "right" to control the processing of personal data.

[30] This approach has long been standard in the legal and policy literature. ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 25 (1971) ("[T]he basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to him—a power that often is essential to maintaining social relationships and personal freedom."); ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) ("Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."); Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) ("Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves."); *see also* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 70–71 (2010).

This control conception can produce peculiar results if and when someone consents to surrender that control. For instance, if Johnny decides voluntarily to strip in front of a webcam with the intention to disclose publicly his personal data, in the form of naked images for all to see and share without any restraints, he is arguably basking in full privacy.[31] That is because the control conception focuses on only the *existence* of control over personal data—not *how* one specifically exercises that control at some given moment. Accordingly, a person who successfully makes his data secluded, confidential, and unknown has no more privacy (in the sense of control) than another who gladly makes his data available to all, on Flickr, YouTube, Facebook, and Twitter.

2. An Alternative Metric: Flow

As an alternative, one could define privacy not in terms of an individual's control over personal data, but in more macro terms that describe the *flow* of categories of personal data within the information ecosystem. In other words, for any particular type of information (e.g., public-record data, medical data, or e-mail contents), one could ask where, how quickly, and with what bandwidth does such information flow, either through push/broadcast or pull/search pathways. Under such a flow conception, public-record data about ourselves, such as whether we voted, flows faster than medical data, which is treated confidentially by law and custom. Put another way, we have less privacy over public-record data compared to medical data.[32]

The flow conception is less focused on a particular individual's exercise of control and more on the data type's flow—how it generally tends to move, as gauged in probabilistic and macro terms, within some information environment. Accordingly, the flow metric can, for example, come to a sharply different measure of privacy for webcam images. If we as a society become sufficiently exhibitionist such that most of us regularly and voluntarily broadcast naked pictures of ourselves on the Internet, our privacy may not have decreased under a control metric. By contrast, the flow

[31] Anita Allen has insightfully explored such weirdness. *See, e.g.*, Anita L. Allen, Commentary, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 867–68 (2000). Allen points out, "You can invade (that is diminish) your own privacy the same way you can diminish your own freedom." *Id.* at 869.

[32] The flow conception has affinities with approaches that define privacy in terms of "constraint on access." *See, e.g.*, ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY 3 (1988) (emphasizing a definition focused on "inaccessibility" of a person to others); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 428–33 (1980) (arguing that privacy is a condition that is measured in terms of the degree of access others have to use through information, attention, and proximity).

of such information will have increased and, conversely, privacy (in the flow sense) will have decreased under the flow metric.[33]

Interesting questions arise from comparing the standard *control* versus the alternative *flow* metric of privacy, and we mean to plant a scholarly flag to mark further inquiry. But those questions do not have to be answered for purposes of this Article. Instead, we offer both conceptions as plausible metrics by which we can more concretely understand and measure privacy, as well as assess privacy proposals. Our case for the PDG, which we detail below, does not strictly depend on which metric one prefers.

B. Privacy Displacement Caused by Self-Surveillance

Having settled on plausible measures of privacy, we turn to the next threshold question: Why should we care about privacy in the first place? After all, if there is no good normative reason, then any claim that self-surveillance undermines privacy should prompt a yawn. One reason to be concerned is that without adequate privacy, those who are privacy anxious will decline to engage in self-surveillance and thus miss out on its benefits.[34] But to answer this question thoroughly, we would need a comprehensive parsing of all other values and countervalues served by increasing or decreasing privacy.[35] For example, if we adopt the control conception of

[33] Our conception also has connections to Helen Nissenbaum's approach to privacy that insists that information flows respect contextual integrity. *See generally* NISSENBAUM, *supra* note 30. Nissenbaum considers privacy to be violated when "[c]ontext-[r]elative [i]nformational [n]orms" are breached without adequate justification. *See id.* at 140. These norms, in turn, can be identified and understood by analyzing various aspects of information flows, including their contexts, actors, attributes, and transmission principles. *See id.* at 150–57. In this nuanced model, an individual's "control" over personal data is not the sole element in deciding whether privacy has been respected, which is similar to the flow approach we offer.

There are, however, differences between our approaches. Nissenbaum's theory of privacy is ambitious in scope. In particular, she seeks to provide both a descriptive and an augmented normative account of privacy. *Id.* at 150. By contrast, we mean intentionally to be more modest and offer no normative account. Moreover, our use of "flow" is meant to be a simpler metric, operationalized closer to the ground, more amenable to mechanical forms of measurement than some violation of a "context-relative informational norm."

To see how our metric differs from Nissenbaum's, suppose that culture changes slowly and incrementally such that most people regularly publicly disclose their GPS trails. In other words, it becomes no big cultural deal. Then, by definition, information would not be flowing beyond expected social contexts. Accordingly, Nissenbaum's contextual integrity might well be preserved and privacy wouldn't be violated, undermined, or decreased. By contrast, according to our flow conception, it doesn't matter that an individual consents or that a culture finds some personal-data practice banal: The GPS information is moving more quickly throughout the information ecosystem, which means privacy over GPS data has indeed decreased.

[34] Dennis Hirsch argues that personal information is a resource that behaves similarly to environmental resources, such as fisheries. Just as over use of the fishery will cause it to collapse, so will over use of personal data by commercial data miners. *See* Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 23–25, 28–30 (2006). This may well be true of self-surveillance data.

[35] For an attempt at some such accounting, see Kang, *supra* note 7, at 1212–20.

privacy, the question for consequentialists would be whether the benefits of increasing individual control over personal data (e.g., encouraging personal experimentation) outweigh the costs of doing the same (e.g., increasing deviant behavior).

As important as such analysis is, that is neither our comparative advantage nor our mission. We instead sidestep this normative conversation—but in a transparent way. Our assumptions are these: The current level of privacy (however measured) is normatively tolerable even if not ideal. However, the advent of self-surveillance will materially decrease the amount of privacy in the near future, holding all other variables constant. That negative privacy displacement can and should be countered such that privacy later is more approximately the same as privacy now.[36] Again, we are not making the normative case for preserving the status quo amount of privacy from first principles or axioms; we are just pronouncing our Whiggish belief.

As a descriptive matter, it should not be controversial to suggest that the advent of self-surveillance will decrease privacy across all, if not most, plausible measures. After all, engaging in self-surveillance means that highly granular Personal Data Streams will be collected. That data then will be uploaded into the "cloud,"[37] as information systems now regularly shunt off data onto remote servers to achieve robustness and flexibility. Increasingly, people have been sharing that data with others in social-media sites, rarely with full comprehension of who can access what. And as such practice becomes more popular, routine, and expected, both social norms and network effects will materially increase an individual's opportunity cost of maintaining her current level of privacy.

Let's return to the CENS Participatory Sensing ("PS") case study.[38] Imagine PS being hosted not by a nonprofit university but by a private-sector firm. As a for-profit venture, this firm has greater incentives to monetize this data in some way, constrained by existing privacy laws and any potential

[36] For some, a more symbolic restatement might help. The following is not actually math, but we provide it just in case it is helpful for some readers. Let p be a privacy function; $p(t_0)$ = privacy at time zero (i.e., right now); $p(t_1)$ = privacy at some future time, t_1. Our prediction is that $p(t_1) < p(t_0)$ because of self-surveillance, holding all other variables constant. We further assume that $p(t_1)$ is less normatively attractive than $p(t_0)$. The goal then is to adopt whatever strategies that will make $p(t_1) \approx p(t_0)$.

[37] "Cloud computing is the style of computing in which the users can rent infrastructure, platform or software services from other vendors without requiring the physical access to them." Karthick Ramachandran, Thomas Margoni & Mark Perry, Clarifying Privacy in the Clouds 3 (Feb. 23, 2011) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1755225_code1383303.pdf?abstractid=1755225&mirid=1. One characterization of cloud computing emphasizes that users simply do not care about the "location" of data or a particular server. *See id.* at 1 ("A main feature of cloud computing is that for operational purposes the cloud users are not interested in their location.").

[38] *See supra* text accompanying notes 12–17.

public-relations blowback.[39] Monetization often means parsing that data for behavioral targeting and advertising, in ways that the average user is unaware. And if and when those data are shared with third parties,[40] the individual will have even greater difficulty exercising subsequent control over how those data flow.

Now, one could respond that self-surveillance could not possibly decrease privacy because the Personal Data Streams will be uploaded pursuant to the terms of an individual's *contract* with some service provider. Put another way, privacy will not decrease in the future because the collection and processing of any and all Personal Data Streams will have been implicitly or explicitly consented to.

This formalistic objection fails for various reasons that are well documented in the literature.[41] Individuals operate under substantial informational and cognitive limitations.[42] Individuals lack perfect information and suffer from information asymmetry about how their data will be used.[43] Individuals make probability-calculation errors and sometimes underweigh harms that are low in salience and diffusely distributed. Individuals suffer from regret, which can be understood as a form of an intrapersonal collective-action problem.[44] At the level of market structure, there may be insufficient competition, bundling of products and services, lock-in and switching costs, etc., all of which contribute to the fact that "control" is exercised only formally.[45]

Finally, as a normative matter, we believe that many readers will share our belief that we should counter the negative displacement in privacy caused by self-surveillance. But to repeat, we attempt no moral,

[39] *See, e.g.*, Caroline McCarthy, *Facebook Beacon Has Poked Its Last*, CNET (Sept. 18, 2009, 11:58 PM), http://news.cnet.com/8301-13577_3-10357107-36.html?tag= mncol;txt.

[40] It's important to recognize that one of those third parties might be the government, such as in some law-enforcement or national-security project. The state can purchase personal data in the marketplace, subpoena it through legal process, or lean hard on private actors in gray cases to get data. *See* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 917–18, 930 (2008).

[41] For a general, skeptical read of how market-based consent operates in cyberspace and information-technology discourse, see Julie E. Cohen, Lochner *in Cyberspace: The New Economic Orthodoxy of "Rights Management,"* 97 MICH. L. REV. 462 (1998). For empirical evidence that individuals rarely read "click-through agreements" or understand them, see Victoria C. Plaut & Robert P. Bartlett III, *Blind Consent? A Social Psychological Investigation of Non-Readership of Click-Through Agreements*, 36 LAW & HUM. BEHAV. (forthcoming 2012).

[42] *See, e.g.*, Paul M. Schwartz, Commentary, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 822 (2000) (identifying the problem of "bounded rationality").

[43] Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CALIF. L. REV. 395, 476 (2000).

[44] *See* CASS R. SUNSTEIN, FREE MARKETS AND SOCIAL JUSTICE 29–30 (1997). There may also be more standard forms of collective-action problems as well. *See* Schwartz, *supra* note 42, at 822.

[45] *See, e.g.*, Schwartz, *supra* note 42, at 823 (raising concerns about the ability to "exit").

philosophical, economic, or policy argument in favor of this normative position.[46] If the reader believes, to the contrary, that there is too much privacy now, then the rise of self-surveillance may cause cheer, not concern.

C. DISTINGUISHING HARDER PRIVACY PROBLEMS

Our final threshold clarification is to point out that in focusing on the domain of self-surveillance, we carve out an easier privacy problem than those raised by other pervasive computing technologies.[47]

1. Not Third-Party Surveillance of Us

First, the problem is *self*-surveillance, not *third-party* surveillance of us. In the standard privacy problem, personal data are collected by some counterparty in the course of an individual's interaction with that counterparty.[48] For example, a brick-and-mortar store collects your image on a video camera as you walk through its aisles, or some electronic merchant collects information about your browsing and purchase habits as you shop online.

Because the counterparty (e.g., the merchant) collects the personal data in the course of interacting (often executing some transaction) with the individual, that counterparty has some plausible claim to the collected information. For instance, because the personal data were collected through the efforts of the counterparty, it often claims to "own"[49] the data in some way.[50] Given such plausible claims, limiting what the counterparty can do with the personal data once collected raises difficult questions sounding in terms of liberty ("It's my data since I collected it!"), efficiency ("Better data

[46] For some such normative account, see NISSENBAUM, *supra* note 30, at 162–64 (describing both "[t]he [v]irtues and [l]imits of [c]onservatism" in the privacy context).

[47] For a general discussion of "pervasive computing," see Kang & Cuff, *supra* note 25; *see also* Dana Cuff, Mark Hansen & Jerry Kang, *Urban Sensing: Out of the Woods*, COMM. ACM, Mar. 2008, at 24.

[48] For an early model of cyberspace transactions that focuses on the individual, "transacting parties," and "transaction facilitators," see Kang, *supra* note 7, at 1223–38.

[49] Given the nonrivalrous nature of information, more than one party can "own" various facts, such as the fact that I bought a red scarf on Tuesday for seventy-nine dollars. I possess that fact in my short-term memory. So does my friend who went shopping with me. So does Victoria's Secret. It is a sort of joint possession. For further discussion of this "entitlement anarchy," see Jerry Kang & Benedikt Buchner, *Privacy in Atlantis*, 18 HARV. J.L. & TECH. 229, 238–41 (2004).

[50] For careful exploration of the relationship between Lockean desert theory and intellectual property, see Seana Valentine Shiffrin, *Lockean Arguments for Private Intellectual Property*, *in* NEW ESSAYS IN THE LEGAL AND POLITICAL THEORY OF PROPERTY 138 (Stephen R. Munzer ed., 2001), where the author argues that Lockean analysis provides a prima facie argument against property rights in intellectual property.

allows me to serve my customers more effectively!"),[51] and freedom of expression ("The First Amendment allows me to communicate and process this data!").[52] Thus, the typical privacy problem poses a collision between an individual's claim over personal data and the counterparty's.

With self-surveillance, however, the counterparty's interest disappears because the counterparty does not exist. Self-surveillance data are not incidentally created and collected when an individual transacts with some counterparty in the public or quasi-public sphere. Rather, these data are created by purposeful, self-initiated surveillance through sensors within the individual's control. Indeed, as a practical matter, these personal data could not be readily collected *but for* the individual's intentional participation in self-surveillance. They constitute approximately a digital version of Ben Franklin's diary. Accordingly, no counterparty (e.g., the merchant in our prior examples) has proprietary claim to such data; it didn't collect the data in the first place and often couldn't (under given technological, legal, and financial constraints) even if it wanted to.[53]

2. Not Our Surveillance of Third Parties

At the same time, self-surveillance is not our surveilling of third parties. To clarify this point, it is useful to distinguish self-surveillance from other pervasive computing technologies, such as Lifelogs.[54] A Lifelog is an attempt to produce a complete multimedia record of one's entire sensory experience for permanent personal archive.[55] Imagine having a video camera on your forehead recording everything you see and hear every

[51] *See, e.g.*, George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 628–33 (1980) (arguing that the more accurate classifications will increase economic efficiency).

[52] *See generally* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right To Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000).

[53] There could be gray areas. For example, what if a third party provides an "app" to an individual to engage in self-surveillance, but that "app" has terms of service that give the third party some proprietary claim to the self-surveillance data. In this context, via a clickwrap contract, the individual has arguably given some proprietary claim to a third party in exchange for self-surveillance assistance. This muddies the sharper distinctions we drew above, which presumed that no such assistance was needed. We concede that contracting away rights to data can always complicate the picture. In some sense, the infrastructure we recommend below, in the form of PDGs and PDVs, is designed to obviate such contracts, such that persons can engage in self-surveillance without significant privacy loss.

[54] For examples of such ventures, see *MyLifeBits*, MICROSOFT RESEARCH, http://research.microsoft.com/en-us/projects/mylifebits (last visited Jan. 16, 2012); *Total Recall: A Personal Information Management System*, USC.EDU, http://bourbon.usc.edu/iml/recall (last visited Jan. 16, 2012).

[55] *See* Martin Dodge & Rob Kitchin, *'Outlines of a World Coming into Existence': Pervasive Computing and the Ethics of Forgetting*, 34 ENV'T & PLAN. B: PLAN. & DESIGN 431, 431 (2007) (defining Lifelog as a "unified digital record of the *totality* of an individual's experiences, captured multimodally through digital sensors and stored permanently as a personal multimedia archive").

second of your waking life.[56] Although it has been characterized as a form of "sousveillance" (in contrast to "surveillance"),[57] a Lifelog for anyone besides a hermit will collect the sight and sounds of other identifiable persons. This is not some "bug" of sousveillance version 1.0; it is instead its central "feature." In this crucial sense, self-surveillance differs from sousveillance. The whole point of self-surveillance is to monitor only the self. By contrast, a Lifelog attempts to record everything that our senses perceive in rich multimedia.

Of course, incidental capture of data about others will take place even within self-surveillance practices. And information about others could be inferred from another person's self-surveillance data.[58] That said, a qualitative difference remains in the quantity and quality of data generated between an inward gaze (capturing data *about oneself*) and an outward gaze (capturing data about others *from one's perspective*). And that difference makes the self-surveillance privacy problem an easier one to solve.

[56] For science-fiction iterations, see THE FINAL CUT (Lions Gate Entertainment 2004).

[57] *See* Steve Mann, *Equiveillance: The Equilibrium Between Sur-veillance and Sous-veillance*, ON THE IDENTITY TRAIL, May 2005, *available at* http://wearcam.org/anonequity.htm. Mann explains,

> Surveillance is derived from French "sur" (above) and "veiller" (to watch). Typically (though not necessarily) surveillance cameras look down from above, both physically (from high poles) as well as hierarchically (bosses watching employees, citizens watching police, cab drivers photographing passengers, and shopkeepers videotaping shoppers).
>
> Likewise Sousveillance, derived from French "sous" (below) and "veiller" (to watch), is the art, science, and technologies of "People Looking at". . . . [S]ousveillance typically involves small person-centric imaging technologies, whereas surveillance tends to be architecture or enviro-centric (cameras in or on the architecture or environment around us). Sousveillance does not necessarily limit itself to citizens photographing police, shoppers photographing shopkeepers, etc., any more than surveillance limits itself along similar lines. For example, one surveillance camera may be pointed at another, just as one person may sousveill another. Sousveillance therefore expands the range of possibilities, without limitation to the possibility of going both ways in an up-down hierarchy.
>
> With the miniaturization of cameras into portable electronic devices, such as camera phones, there has been an increased awareness of sousveillance (more than 30,000 articles, references, and citations on the word "sousveillance" alone), and we are ready to see a new industry grow around devices that implement sousveillance, together with a new sousveillance services industry.

Id. See generally Steve Mann, Jason Nolan & Barry Wellman, *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*, 1 SURVEILLANCE & SOC'Y 331, 332 (2003) (discussing the difference between sousveillance and surveillance).

[58] For example, if one has a young child, it will be easy enough to infer her location in a morning commute to school from the parent's location.

IV. A NEW APPROACH: THE PERSONAL DATA GUARDIAN

So far, we have just cleared brush. First, we identified a nascent socio-technological practice of self-surveillance. Second, we described how this practice will decrease the net amount of privacy, measured in plausible ways. Third, we stated our normative assumption that this net loss is unattractive. If lawmakers and policymakers agree, how might they counter the displacement?

Mandatory laws prohibiting or limiting self-surveillance seem exceedingly unwieldy and unlikely. After all, in modern American culture, how feasible is it for the government to say that you cannot measure yourself? Another predictable response is to suggest some technological fix, which typically touts encryption and efficient individual-preference expression. But so-called privacy-enhancing technologies by themselves—without supporting structures—have historically failed.[59] Finally, there will be those who argue in favor of self-regulation although that means embracing the status quo and its predictable privacy displacement. We suggest a novel structural strategy: We call forth the Personal Data Guardians ("PDGs").

A. *PERSONAL DATA GUARDIAN*

Our strategy is to introduce into the information ecosystem a new species, which functions as a professional intermediary between the individual client and those who would process the client's self-surveillance data. Specifically, we seek to jumpstart the creation of the PDG, whose principal mission is to maintain a digital storage locker called a Personal Data Vault ("PDV"). An individual client would upload her Personal Data Stream into that PDV, maintained by her PDG, instead of into some amorphous cloud owned and operated by some faceless third party.

1. Role Ideology

The PDG would embrace a professional identity of expertise and service, as has been done by other professionals such as lawyers, accountants,

[59] *See, e.g.*, A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1524 (2000) (describing privacy-enhancing technologies as insufficient to meet the evolving challenges presented by developments in personal-data-collection technology); Bert-Jaap Koops & Ronald Leenes, *'Code' and the Slow Erosion of Privacy*, 12 MICH. TELECOMM. & TECH. L. REV. 115, 187 (2005) (questioning the efficacy of privacy-enhancing technologies as "[t]hey remain a mainly theoretical solution that has yet to prove [their] effect in practice"); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1126 (2000) (arguing that privacy-enhancing technologies "have thus far done little to make cyberspace more privacy-friendly"). For a similar skeptical view, as applied to cloud computing, see Ramachandran, Margoni & Perry, *supra* note 37, at 5.

financial planners, and librarians. Their role ideology[60] would include the core idea of acting as trustworthy confidantes on behalf of their clients (vis-à-vis third-party snoops, subpoenas, and government surveillance), zealous advocates who negotiate for best informational terms vis-à-vis third-party application service providers (3P-ASPs), and wise counselors to their individual clients about their decisions regarding self-surveillance data.

2. Professional Self-Regulation

The PDG would be an individual human being, licensed as a professional by a state self-regulatory body, which would be most easily created by state statute.[61] This professional association would adopt minimum standards to enter into the profession, which could include infrastructural capacity as well as technological, legal, and business competence, and minimum requirements of continuing education. The association would also adopt internal model rules of ethical and professional behavior, whose violation could lead to enforcement actions by the disciplinary arm of the association as well as malpractice suits by clients. Following the analogy with lawyers, PDGs could partner with other Guardians to create a firm—in a general partnership or in a limited liability partnership.

B. PERSONAL DATA VAULT

The Guardian would maintain the PDV, a sort of digital safe-deposit box for self-surveillance data.[62] It should provide three basic functions: secure storage, user legibility, and guided third-party access.

1. Secure Storage

The Personal Data Stream collected through self-surveillance would be securely uploaded for storage in the PDV. PDVs can be large and physically distributed, hosted across multiple servers. Hosted PDVs can provide a level of secure storage, robustness, and ease of backup that storing data locally could not provide.[63]

[60] For a discussion of "role ideology," see Sung Hui Kim, *The Banality of Fraud: Re-Situating the Inside Counsel as Gatekeeper*, 74 FORDHAM L. REV. 983, 1012 (2005).

[61] The licensing system could also occur at the federal level via congressional statute and supervision by some federal agency such as the Federal Trade Commission. That said, professionals are more typically regulated on a state-by-state level. We also think it more likely that a state legislature, rather than Congress, could be persuaded to experiment with a PDG model.

[62] For technical details and descriptions, see Min Mun et al., *Personal Data Vaults: A Locus of Control for Personal Data Streams*, *in* PROCEEDINGS OF THE 6TH INTERNATIONAL CONFERENCE (2010), *available at* http://dl.acm.org/citation.cfm?id=1921191&bnc=1.

[63] At a minimum, PDVs must include secure storage, methods for managing individual and third-party identities, access control, selective sharing, ability to perform some computation within the vault, data management and audibility, data-visualization interfaces, and service

2. User Legibility

The personal data stored in the PDV belongs to the individual. But what might it mean for the average individual to access her own data when digital strings of ones and zeros mean nothing to the typical human being? In some sense, that data has to be made legible to the individual, which means that it must be visualized. We believe that legibility should include visualization of the data in the form of basic descriptive and correlational statistics, as well as visualization across the dimensions of space and time. In other words, basic legibility should allow simple mash-ups with geospatial data through the use of Geographic Information Systems tools. In addition, Guardians should provide some basic facility to represent the data across time, to show time series and trending. We expect this basic legibility standard to evolve over time, as new techniques emerge from the data-analysis community, Guardians, or even users themselves.

3. Guided Third-Party Access

Individuals, of course, seek more than basic legibility. They desire more refined applications provided by commercial and noncommercial 3P-ASPs. The PDV structure will allow individuals to work with 3P-ASPs in flexible and granular ways, instead of opting for an all-or-nothing divulgement of raw self-surveillance data. First, the data might never have to leave the PDV since the PDG can simply apply 3P-ASPs' scripts to the data and forward only the output to the client.[64]

interfaces to integrate with third parties. The data store should be redundant to prevent data loss and should track data provenance and log access to the data. It should also track user changes to sharing rules over time. While the PDV can support strong identity that links data to a unique individual (the data owner), it may also support anonymous and pseudonymous sharing by preventing third parties from cross-referencing multiple streams to determine identity. There are numerous technical issues involved in delinking identity from data. These include authenticating both user and third-party applications, separating personally identified information from data streams, and managing when and how user identity is shared with third-party applications. PDV designers will need to consider how users are identified to the PDV operator and how authentication of data captured on a handset is accomplished, so that malicious parties may not send unauthorized data to the PDV. If personally identifiable information (e.g., name, address, etc.) is held by the PDV, it might be kept apart from the data itself to protect against internal meddling by PDV employees or, in some cases, subpoena. The PDV and compliant third parties can encourage users to participate in services without those services requiring the identity of the user. This might require a service-specific method of utilizing pseudonyms as part of the PDV API.

[64] By hosting some computation within the vault and exporting only outputs, individuals can access detailed and accurate application outputs while protecting detailed personal information. The simplest way to do so is to install common computations as built-in libraries to the PDV. Several types of processing are in common use across Participatory Sensing applications. One example is inferring transportation modes such as walking, running, biking, and driving using accelerometer and GPS data. Another example is transforming GPS data to place name, city name, ZIP code, region name, and country name. This approach resolves the

Second, if information must be provided to the 3P-ASP, the PDG would adhere to a parsimony principle that discloses the least amount of data necessary to execute the requested analysis. Accordingly, she might provide only summary statistics (not the raw data), a subset of data,[65] or filtered data.[66] When any such data do leave the PDV, the PDG can scrub and pseudonymize the data.[67] Along the way, the Guardian would be expected to exercise her own expert judgment and make recommendations on behalf of her clients about various personal data-sharing strategies, including which third parties to trust. All of these data transactions could be electronically audited as part of good security.[68]

C. *LEGAL RELATIONS*

The fundamental relationship between the individual client and the PDG would be that of the common law's principal and agent, which would mean that the PDG owes fiduciary duties to her client in handling her self-surveillance data. Consistent with this arrangement, three important duties must be respected.

issue of running untrusted application code inside the PDV, and the extent of data sharing choices can be limited by built-in libraries.

[65] The PDG can identify the minimum data type and sampling rate needed by a 3P-ASP and share only that minimum type and amount. For example, the PDG might release GSM cell-tower triangulations rather than more precise GPS data to third-party applications that don't require fine-grained location information. Or the PDG could release only the amount of time spent driving if the actual position is not necessary.

[66] Selective access could use filters that can share or protect data based upon variables such as time, activity, and nature of third-party requests. These could include warning systems. Filters could make it easy for individuals to express data-sharing preferences (e.g., share data only collected between 8 a.m. and 10 a.m.; share data only when I am driving; or share data only with my doctor). Adaptive filters could learn from user data and use anomaly detection to further help users manage the logistical burdens of selective sharing. For instance, an unusual trip to buy a present for a spouse might be flagged by the PDV, prompting the user to deny access to that single trip to a third-party application.

[67] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1744–45 (2010) (proposing for legal discourse the term *scrub* instead of *anonymize* or *deidentify*). Ohm points out that reidentification of "anonymized" data has been shown to be much easier than commonly supposed. *See id.* at 1716–27.

[68] Users or external auditors should be able to audit an application provider's storage and access practices and their use of private data to ensure that it abides by published privacy policies. Moreover, applications might provide tools for users to explore their trails: where and when data originated, what processes were performed on that data, and if and when data was shared. Such tools could become complicated because the volume of audit information scales as a user provides more access to their data. For auditing to be effective and to reduce consumer confusion, it may be necessary to have auditing agencies (analogous to credit-reporting agencies or rating agencies). Maintaining per-access audits for each user across several PDVs and providing fast analyses of audit trails raise technical research challenges to explore.

1. Fiduciary Duties

As a faithful agent, the Guardian must demonstrate a minimum competence in terms of safely storing, securing, deleting, analyzing, and presenting (making legible) an individual's self-surveillance data. This *duty of care* could be enforced through internal-to-the-profession disciplinary action and the standard common-law malpractice tort.

Just as a lawyer or accountant may not ordinarily reveal client confidences, the same would be true with the Guardian. This *duty of confidentiality* could be enforced through disciplinary action, as well as tort[69] or contract actions.

Finally, as a fiduciary, the Guardian owes a *duty of loyalty* to the individual client. But conflicts of interest can arise if the Guardian becomes vertically integrated with 3P-ASPs. In such cases, what is best for the individual client may not be best for the PDG, who could profit from the individual's adoption of her own application services. Instead of monitoring for misbehavior, which has historically been difficult in such contexts, an ex ante structural solution would be cleaner. Just as we don't generally allow law firms to provide vertically integrated services and thus prohibit attorneys from partnering with non-attorneys in multidisciplinary practices,[70] the Guardian would be similarly quarantined from providing application services.[71]

2. Evidentiary Privilege

In addition to the above three fiduciary duties, an *evidentiary privilege* similar to the noncommercial trade-secret privilege would protect the self-surveillance data stored in the PDV. In other words, none of the data stored in the PDV could be subpoenaed or introduced into any legal proceeding unless the privilege was waived by the individual or subject to some clearly delimited exception.

Similar to the three duties discussed above, this privilege could be recognized by state-judge extension of the common law. Some analogies can be found, for instance, in the recognition of a self-evaluation or self-critical analysis privilege in certain states.[72] In the alternative, state legislatures[73]

[69] The tort could be malpractice. In addition, common-law courts could recognize a separate cause of action for breach of confidentiality.

[70] Model Rule of Professional Conduct 5.4 prevents nonlawyers from partial ownership of a law firm. It also prevents lawyers from providing multiple services (beyond legal services), such as accounting or healthcare, from the same office. MODEL RULES OF PROF'L CONDUCT R. 5.4 (2005).

[71] Model Rule of Professional Conduct 5.7 permits law firms to own other lines of business through structurally separate arms. *Id.* R. 5.7. We are skeptical that structural separation would suffice.

[72] Some such privileges have been recognized in the context of medical committee reports, affirmative-action studies, and environmental-impact assessments. *See, e.g.*, James F.

could pass a statute creating the privilege, as some have done for medical committee reports.[74]

a. The Need for the Privilege

This evidentiary privilege provides substantial benefits to individuals engaging in self-surveillance. Currently, such data, wherever it is held, is subject to civil discovery requests. For example, in federal litigation, the Federal Rules of Civil Procedure provide that "[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense."[75] Furthermore, "[r]elevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence."[76] Given this broad scope of discovery, parties in divorces, contract disputes, and tort actions can subpoena self-surveillance data, which is now typically held by third parties.

Consider, for example, the case of *Ledbetter v. Wal-Mart Stores, Inc.*, in which plaintiffs Heath and Disa Powell sued Wal-Mart for injuries and loss of consortium allegedly suffered due to an electrical accident that occurred while one of the plaintiffs was fixing an electrical system in an Aurora, Colorado, Wal-Mart.[77] The alleged injuries included "sleep disturbance and anxiety" as well as "fatigue, cognitive inefficiencies and depression," all contributing to claims for direct damages as well as to the claim for loss of consortium.[78]

Wal-Mart issued subpoenas to MySpace, Facebook, and Meetup.com, hoping to uncover information and communications stored by these websites that would refute the plaintiffs' medical diagnoses and cast doubt

Flanagan, *Rejecting a General Privilege for Self-Critical Analyses*, 51 GEO. WASH. L. REV. 551, 552 (1983) (suggesting that protection for self-critical evaluations has been found in only three contexts: peer reviews, affirmative-action studies, and internal corporate investigations); S. Kay McNab, Note, *Criticizing the Self-Criticism Privilege*, 1987 U. ILL. L. REV. 675, 678–82 (describing doctrinal evolution of self-criticism privilege).

[73] We focus on state legislatures because although Federal Rules of Evidence Rule 501 gives the federal courts broad discretion in applying privileges "in the light of reason and experience" within the federal courts, Congress expressly rejected the adoption of any specifically enumerated privileges. CHARLES ALAN WRIGHT & KENNETH W. GRAHAM, JR., FEDERAL PRACTICE AND PROCEDURE: EVIDENCE § 5421, at 587 n.79 (Supp. 2008); *id.* at 648 (1980). Federal courts generally apply the privilege law of the states in which they sit.

[74] *See, e.g.*, Gail N. Friend et al., *The New Rules of Show and Tell: Identifying and Protecting the Peer Review and Medical Committee Privileges*, 49 BAYLOR L. REV. 607 (1997) (describing Texas privileges for peer review and medical committees).

[75] FED. R. CIV. P. 26(b)(1) (2010).

[76] *Id.* Many states have similarly broad discovery standards. *See, e.g.*, CAL. CIV. PROC. CODE § 2017.010 (West 2007); COLO. R. CIV. P. 26(b)(1) (West 2010); KAN. STAT. ANN. § 60-226(b)(1) (2010); N.Y. C.P.L.R. § 3101 (McKinney 2005); WYO. R. CIV. P. 26(b)(1) (2011).

[77] Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2009 WL 1067018 (D. Colo. Apr. 21, 2009); *see* First Amended Complaint and Jury Demand at 3, 8–9, *Ledbetter*, 2009 WL 1067018.

[78] *Ledbetter*, 2009 WL 1067018, at *1.

on the loss-of-consortium claim.[79] When third-party websites are served subpoenas in civil litigation, they typically put up at least mild resistance as a matter of internal policy. However, "privacy policies" make clear that they will turn over data when lawfully required to do so. Being served a subpoena is part of that lawful process.

One might believe that specific privacy laws, such as the Stored Communications Act,[80] prevent such disclosure. Indeed, citing this Act, the various websites subpoenaed in the *Ledbetter* case declined Wal-Mart's request for information.[81] This just led Wal-Mart to file a motion to compel discovery against the plaintiffs who, according to Wal-Mart, had "possession, custody, or control"[82] over the relevant information because they could grant or deny access to their accounts. Agreeing with this characterization, the court compelled the plaintiffs to grant the social-networking websites permission to disclose the requested information to Wal-Mart.[83] We believe that such discovery motions will become common practice. The results would differ radically if the self-surveillance data were held within a PDV, protected by something like a trade-secret privilege.

b. The Mechanics of the Privilege

To make our analysis concrete, imagine that as part of a PDG initiative, a state legislature creates the following privilege:

> An individual has a privilege, which may be claimed by him/her to refuse to disclose and to prevent other persons from disclosing self-surveillance data stored in a Personal Data Vault by a licensed Personal Data Guardian, so long as the allowance of the privilege will not tend to conceal fraud, enable criminal activity or otherwise work injustice. When disclosure is directed, the judge shall take such protective measure as the interests of the holder of the

[79] *Id.* Self-authored text and manually uploaded photographs and videos of oneself are in some sense primitive forms of self-surveillance. However, these social sites could include applications, for example, that include location streams, which fit squarely into the definition of self-surveillance data.

[80] Stored Communications Act, 18 U.S.C. §§ 2701–2712 (Supp. 2010).

[81] Defendant Wal-Mart Stores, Inc.'s Motion To Compel Production of Content of Social Networking Sites at 2, *Ledbetter*, 2009 WL 1067018.

[82] *Id.* at 5–6. Federal Rule of Civil Procedure 34 states that this requirement applies to "any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recording, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form." FED. R. CIV. P. 34(a)(1)(A) (2010).

[83] *Ledbetter*, 2009 WL 1067018, at *2.

privilege and of the parties and the furtherance of justice may require.[84]

Evidentiary privileges are either topical or communicative. In other words, they protect either information on a certain subject matter (e.g., trial-preparation materials)[85] or confidential communications between two people (e.g., attorney–client). The self-surveillance privilege is designed to be the former, since we are interested in protecting the underlying observations collected through self-surveillance and not just the confidential communication[86] between, say, the individual client and the PDG.

Topical privileges, including this one, might seem overbroad because they are not constrained to the confidential communications between two select parties. But notice that this privilege is limited in terms of scope and strength.

i. Scope

First, as a matter of scope, the privilege only protects "self-surveillance data" that is stored in a PDV maintained by a licensed PDG. Accordingly, if an individual simply recorded herself and kept the data on her own computer, it would not benefit from the privilege because a PDG is not holding the data.[87] Critics may challenge this sharp limitation of the privilege: after all, if the goal is to protect a sort of information, why should it matter who happens to be holding it? This is a fair point, but we advocate a bright-line rule to discourage overbroad assertions of the privilege. When an individual claims the privilege, she may be inclined to do so self-servingly. By interjecting a PDG as an intermediary, who has professional responsibilities, the privilege is less likely to be abused.

ii. Qualified Privilege

Second, as a matter of strength, the topical privilege is far from absolute. The proposed statute states explicitly that the privilege may not be deployed to "conceal fraud, enable criminal activity or otherwise work

[84] This text is modeled after the Federal Rules of Evidence Rejected Rule 508 proposing a trade-secrets privilege.

[85] *See* FED. R. CIV. P. 26(b)(3) (also known as "work product").

[86] Unlike the topical privileges that protect facts, a confidential-communications privilege applies only to communications. According to Imwinkelried, "communication[s]" include "expressive statements and acts." EDWARD J. IMWINKELRIED, THE NEW WIGMORE: A TREATISE ON EVIDENCE: EVIDENTIARY PRIVILEGES § 6.7.1, at 731 (Richard D. Friedman ed., 2d ed. 2009). A statement or act "is expressive if the speaker or writer subjectively intends the statement to convey meaning to a person such as a hearer or reader. . . . [S]tate of mind must also exist at a particular time. . . . [T]he transfer of a pre-existing document does not qualify the document for protection." *Id.* at 731–32 (citations omitted).

[87] We could envision allowing local backup copies of the PDV (a reverse-cloud backup), for example on separate hard drives, as long as it remains within the networked "custody" of the PDG.

injustice."[88] Further, as characteristic of qualified privileges, every attempt to establish a self-surveillance data privilege would need to pass a case-by-case balancing test at the discretion of the trial judge.[89] The privilege would not give way just because some of the self-surveillance data is "generally relevant" to a party's case or claim.[90] As such, it would effectively stop discovery requests that reflect bad faith, maliciousness, or unnecessary prying.[91] Rather, the judge would override the privilege only if the self-surveillance data are "*directly relevant* to a *material element* of the cause of action (or defense) *and necessary* because the party opposing the claim of privilege would be *unfairly disadvantaged* in proving its case absent access to the" self-surveillance data.[92] And when they do so, judges would take care to use techniques such as *in camera* review or protective orders to limit public disclosure of the evidence.

D. COMPARISON AND CONTRAST

It might be useful to compare our PDG proposal with other calls for information intermediaries in the privacy literature. For example, in the late 1990s, John Hagel and Marc Singer called for the creation of an infomediary who would mediate between the individual and the marketer.[93] The infomediary would be privy to an individual's preferences and would actively research ways to satisfy those preferences at the lowest cost while at the same time protecting personal information from marketers.[94] In 2006, Eric Goldman called for an automated variation on this theme, which he called "Coasean filters."[95] These would be intelligent software agents residing on our mobile phones that would automatically collect highly granular information about our preferences by monitoring our behavior and transactions. These filters would be maintained by third-party vendors, which may or may not have access to the raw data collected but would likely

[88] *See supra* text accompanying note 84.

[89] *See* WRIGHT & GRAHAM, *supra* note 73, § 5421, at 663–64 n.73 (1980). The "trial court [has] discretion to override the privilege claim whenever the factors that support the privilege claim are outweighed by some countervailing factor or factors." *Id.* § 5650, at 384 (1992) (citation omitted). Factors that the trial judge would weigh include: dangers of abuse, good faith, adequacy of protective measures, and availability of other means of proof. *Id.* at 386–87.

[90] *See, e.g.*, WILLIAM E. WEGNER ET AL., CALIFORNIA PRACTICE GUIDE: CIVIL TRIALS AND EVIDENCE 8E-149 (2010) (internal quotation marks omitted).

[91] *See, e.g.*, WRIGHT & GRAHAM, *supra* note 73, § 5650 (1980).

[92] *See* WEGNER ET AL., *supra* note 90, at 8E-149.

[93] *See* JOHN HAGEL III & MARC SINGER, NET WORTH: SHAPING MARKETS WHEN CUSTOMERS MAKE THE RULES 28–29 (1999).

[94] *Id.* Also, when Kenneth Laudon called for a National Information Market, where individuals would deposit personal data in bank-like "accounts," he noted the possibility that "information fiduciaries" would emerge. *See* Kenneth C. Laudon, *Markets and Privacy*, COMM. ACM, Sept. 1996, at 92, 99–101.

[95] *See* Eric Goldman, *A Coasean Analysis of Marketing*, 2006 WIS. L. REV. 1151, 1202 (internal quotation marks omitted).

receive some, perhaps anonymized, data stream in order to make inferences about the individual and her preferences.[96]

In these infomediary proposals, the basic goal is to create an entity that leverages technology to decrease the costs of matchmaking between individual privacy preferences and third-party marketers. Our PDG proposal differs in two material ways. First, the fundamental purpose of the PDG is not to facilitate commerce by profiting from a two-sided market of merchants and individuals. Instead, the much narrower goal is to protect self-surveillance data. Put another way, the goal of the PDG is not to minimize transaction costs of online shopping by facilitating targeted advertisements. Instead, the role ideology of the PDG is to intentionally and mindfully slow down data flows, advise the individual of unexpected consequences, and adopt default best practices that are in the individual's best interests.

Second, the PDG is bound by law to the individual in a fiduciary relationship. Moreover, it is barred from other lines of business in order to avoid predictable conflicts of interest. By contrast, the infomediaries envisioned by prior commenters were not so constrained. They functioned more as commercial middlemen than as trustee or faithful agent. One of the reasons why such intermediaries never came into existence was because there was little reason to trust these middlemen. Why would an individual concerned enough about privacy to seek out a privacy intermediary allow some third party to have plenary access to his personal data without some legal guarantees?[97]

* * *

We have provided only a cursory sketch of the PDG, but the payoffs for privacy should be clear. For example, under the control metric of privacy, having an expert and loyal agent will likely increase an individual's actual (as opposed to purely formal) control over personal data. Consider by analogy a similar relationship in the context of medicine. Having an expert and loyal doctor surely increases our control (actual autonomy) over our own bodies. We reach a similar conclusion with the flow metric of privacy. By role ideology, a PDG is invested in slowing down—not speeding up—the flow of personal data. Professional ideology, as well as fiduciary law, require her to put her clients' interests above that of third parties. Moreover, the Guardian is structurally conflicted out of adjacent vertical markets, which decreases the chance that financial self-interest will warp recommendations.

[96] *See id.* at 1211, 1214–15.

[97] There is one other similarity worth pointing out. Goldman called for an attorney-client-like privilege for vendors who provided "Coasean filters." *See id.* at 1216. Our proposal also calls for a privilege; however, we prefer a trade-secret-like privilege, which is a topical and not a communicative privilege. The goal is to protect the underlying facts collected through self-surveillance and not just the communications between individual and intermediary.

V. OBJECTIONS

A. IMPLAUSIBLE?

So, how precisely will this PDG come into existence and be used? One could imagine them being legally mandated in certain circumstances. By way of analogy, in various states, one cannot consummate a real-estate transaction without the participation of either real-estate agents or lawyers. In various countries, one cannot create a priority claim to loan collateral without the participation of a civil law notary.[98] In other words, by force of law, an intermediary is injected into a market transaction that makes it impossible or difficult for two parties to interact otherwise. For the most sensitive self-surveillance data (e.g., genetic or medical),[99] this

[98] *See* Patrick Del Duca, *Why Some Civil Law Systems Burden Notice-Filing with a Civil Law Notary "Public Writing" Requirement*, 44 UCC L.J. (forthcoming 2011) (manuscript at 5–6). In contrast to notaries in the United States, civil law notaries receive specialized training beyond that of lawyer and generally enjoy higher status and compensation than lawyers. *See id.* at 2–3.

[99] At various moments, we've raised the domain of medical data. One might naturally wonder whether certain medical-privacy laws might apply to the PDV. In particular, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule "protects the privacy of individually identifiable health information." *Health Information Privacy*, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/index.html (last visited Jan. 16, 2012). For HIPPA, see 45 C.F.R. §§ 160, 164 (2010). But it applies only to such information held by three types of entities: health plans, healthcare clearinghouses, and certain healthcare providers. *See id.* § 160.102(a); *id.* § 160.103 (defining "covered entity"). Under the HIPAA Privacy Rule, a health plan is "an individual or group plan that provides, or pays the cost of, medical care," and a healthcare provider is "a provider of services . . . , a provider of medical or health services . . . , and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." *Id.* § 160.103. Neither of these definitions applies to the PDV system, which merely stores (and transmits) self-analytic data. A storage-only PDV also does not qualify as a "health care clearinghouse," defined by the HIPAA Privacy Rule as a:

> public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:
>
> (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
>
> (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Id. Because the PDV stores but does not process data, nor acts as an intermediary between health plans and healthcare providers, it cannot be classified under the rule as a healthcare clearinghouse. Were the PDV system to process raw self-analytic data into a standardized format for the benefit of the user, the HIPAA Privacy Rule would still not apply because the PDV system is receiving the data from the individual and the individual determines where this data is transferred. A system somewhat analogous to the PDV system, and which is also not regulated by HIPAA, is Google Health (http://www.google.com/health), a free service designed by Google to "store [and] manage . . . all of your health . . . information in one central [online] place." *About Google Health*, GOOGLE HEALTH, http://www.google.com/intl/en_US/health/

intermediation could be made an immutable legal requirement. But that is not our general recommendation. Instead, we propose that the law merely create the PDG profession and indirectly catalyze voluntary relationships between them and their clients.

Accordingly, we need to provide some plausible business case for PDGs. Put another way, we need to explain why individual clients might purchase PDG services at a price that would make it worthwhile for the Guardians to enter the profession.

1. Plausible Price Points

Any prediction in law reviews about whether an entire line of business is economically viable will, of course, be speculative. That said, some rough comparisons on costs can provide useful information. For instance, consider what various software and storage services cost in 2011. In terms of secure storage, mozy.com offers 50 GB of personal backup storage for approximately $70 per year.[100] In terms of privacy-promoting services, web anonymizer proxies, such as Anonymizer.com, charge $80 per year.[101] Identity-theft protection services, such as Lifelock, (claim to) guard against identity theft and assist clients who are victimized for $110 per year.[102] Wells Fargo offered a "vSafe" account, advertised as "Your Personal Online Safe," that allowed storage of 1 GB of data for $4.95 per month. [103] It seems plausible, then, that a Guardian could offer basic PDV services to individual clients at approximately $100 per year, which we believe would be inexpensive enough for many individuals to sign up.[104]

about/index.html (last visited Nov. 16, 2011) (Google Health has been discontinued as of Jan. 1, 2012). The PDV and Google Health systems are similar to the extent that both may store self-analytic healthcare information and both serve individuals. However, unlike the PDV system, Google Health's specific purpose is to store all healthcare information, and it does not store non-health related self-analytics. In contrast, the PDV system is designed to store all self-analytics and exclude non-self-analytic healthcare information. On its site, Google Health states: "Google Health is not regulated by [HIPAA]. . . . because Google does not store data on behalf of health care providers. Instead, our primary relationship is with . . . the user." *Google Health Privacy*, GOOGLE HEALTH, http://www.google.com/intl/en_US/health/about/privacy.html (last visited Jan. 16, 2012).

[100] *See* MOZY.COM, https://mozy.com/home/pricing/ (last visited Jan. 16, 2012).

[101] *See* ANONYMIZER.COM, http://www.anonymizer.com/homeuser (last visited Jan. 16, 2012).

[102] *See Enrollment*, LIFELOCK.COM, https://secure.lifelock.com/enrollment/ (last visited Jan. 16, 2012).

[103] *See Wells Fargo vSafe® Frequently Asked Questions*, WELLS FARGO, https://wellsfargo.com/help/faqs/wellsfargovsafe (last visited Jan. 20, 2012).

[104] We recognize the class implications of any market-based solution. Those with less income will be less likely to pay for a PDG. There is, however, some self-selection amelioration. Individuals who cannot afford a PDG solution are more likely to be the same people who can't afford to engage in self-surveillance.

2. The Value of Security and Privilege

What's the value proposition for that price? Already, many of us throw data (both self-surveillance and not) up into the "cloud"—our genetic information here, our GPS data there, our photos here, our house energy usage there—with nothing but generic privacy statements on webpages and clickwrap licenses. Some of us do so without any concern whatsoever about privacy. However, many of us do so with a vague anxiety that something bad might potentially happen, but without a feasible alternative, we adopt a fatalistic attitude towards what seems like an inevitable loss of privacy. Think how much more comfortable we might be if all such data were as safe as if they had been delivered to a professional trustee whose sole job was to safeguard that data.

Of course, no technological or legal safeguard is foolproof. Evidentiary privileges can be pierced, and malpractice actions against professionals who make mistakes are burdensome. But our pitch would always be: "Compared to what?" Having some protection is better than none.[105] And the only way to get this benefit, given the way that we have designed the privilege, is by depositing one's self-surveillance data with a licensed PDG.

3. The Value of Education and Guidance

In addition to secure and privileged storage, PDGs could teach and advise. After all, the point of self-surveillance is increased self-knowledge. This requires some education, exposure to statistical concepts, and understanding of inferences. Just as the best financial planners help their clients understand concepts such as portfolio diversification, the time value of money, tax deductions (too often confused with credits), and compound interest, Guardians might do the same for their clients. By this we don't mean personally customized one-to-one tutorials, which probably would be too expensive.[106] Instead, we mean something like the financial-literacy

[105] A skeptic might say that if it is an Internet data service that doesn't provide immediate gratification (e.g., music, games, pornography), customers won't pay for it, and instead insist on free services financed by advertisements. Obviously, we are not sanguine about the idea of a PDG delivering ads to her clients. One solution might be to sell clients a physical object, such as a hard drive, on the assumption that consumers are more willing to pay for such items. One could imagine PDGs selling hard drives that offer local encrypted backup of their PDVs. As self-surveillance data are streamed to the PDG, they could be sent back down to a specifically authenticated drive in a reverse-cloud backup. The cost to the PDG of the drive might be $100. But PDGs could sell them to their clients as part of their service for $200, thus producing the $100 markup necessary to provide their services. This is sheer marketing speculation. We thank Jeff Jonas for conversations about this idea.

[106] That said, there may be varying tiers of service amongst PDGs. We don't mean to cap the quality of education or service they can provide, except to prevent them from vertically integrating into adjacent services.

training provided by The Motley Fool through its website,[107] or the educational materials on the nonprofit Privacy Rights Clearinghouse[108] and the Electronic Privacy Information Center.[109]

4. The Value of a Legally Secured Fiduciary Relationship

Finally, it's important to remember that the law has secured a fiduciary relationship. True, third parties could offer to do the same via contract. But one would need legal training to distinguish between advertising puffery and actual legal relations. An illustrative example comes from Wells Fargo's vSafe product. In its advertising, Wells Fargo promises safety and security. But in its actual terms of service, Wells Fargo states in fine print: "You acknowledge that by storing copies of your electronic records with us, no fiduciary relationship is created between you and us."[110] Furthermore, no amount of private contracting could replicate the evidentiary privilege discussed above. Finally, one would have more recourse against an incompetent or disloyal Guardian than a third party. Besides the contract claim, a client would be able to sue a PDG in tort as well as initiate some self-regulatory disciplinary action.[111]

5. Other Market Contingencies

a. Changing Social Norms

We note two further ways to influence the market viability of PDGs. First, consider a world with different social norms. Imagine a world where it would seem uncouth, unsafe, and downright shady for a third party to ask an individual directly for her self-surveillance data. It could be akin to an Internet merchant insisting on your social security number to make a minor purchase. An individual might think to herself: "Why would they do that

[107] MOTLEY FOOL, http://www.fool.com (last visited Jan. 20, 2012). The site's trademarked motto is, "The Motley Fool: To Educate, Amuse & Enrich." *Id.*

[108] PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org (last visited Jan. 20, 2012).

[109] ELECTRONIC PRIVACY INFO. CTR., http://epic.org (last visited Jan. 20, 2012).

[110] WELLS FARGO, WELLS FARGO VSAFE® SERVICE AGREEMENT 2 (2008), *available at* https://www.wellsfargo.com/downloads/pdf/wfonline/vsafe_service_agreement.pdf. Further, there is no evidentiary privilege. The Agreement states: "You understand that we may provide copies of electronic records in your *Wells Fargo vSafe* Account and our audit logs in response to legal process." *Id.* at 5.

[111] We don't want to be overoptimistic about self-regulation. We recognize that professional societies serve as only mild deterrents to bad behavior. *See* Richard L. Abel, *United States: The Contradictions of Professionalism, in* 1 LAWYERS IN SOCIETY: THE COMMON LAW WORLD 186, 188 (Richard L. Abel & Philip S.C. Lewis eds., 1988) ("American lawyers pursued the project of market control through their professional organizations, and they justified those institutions by the axiomatic identification of professionalism with self-regulation. But the actual experience of self-regulation has tended to undermine the profession's claim to privileged immunity from external oversight."). But mild deterrence is better than nothing.

when a perfectly functioning data vault system exists? What are they trying to do?" And if a corps of Guardians do come into existence, fully embrace their role, and evangelize accordingly, then social norms could emerge strongly against directly depositing self-surveillance data with less trustworthy third parties. Admittedly, this poses a chicken-and-egg problem: We might need PDGs to help produce such social norms, but such social norms might be necessary for people to want PDGs. Our point is that if PDGs come into existence and get some traction, there may be positive feedback loops that encourage their growth and viability.

b. Government Contracts

Second, consider how the government might exercise market power indirectly to improve PDG economies of scale. Academic research institutions that receive government funding through grants and contracts form a significant market for personal data. These institutions are governed by strict national guidelines for the protection of research subjects.[112] Researchers concerned about mandates of respect, beneficence, and justice for research subjects might use PDGs to promote meaningful consent and minimal harm, two tenets of research ethics.[113] PDVs would allow research subjects to collect study data and then submit that data to participating researchers trusted by PDGs. Researchers working on particularly sensitive issues might run federated queries with the PDVs, thereby gaining access to aggregate statistics without accessing the raw data themselves. PDVs could help researchers gain approval from their Institutional Review Boards ("IRBs") and comply with national guidelines for the protection of research subjects. Incentives for research participants might grow to include funding for PDV subscriptions, much as sensing-research incentives currently include access to mobile phones and data plans.

c. Third Party Buy In

The possibility of such federated queries might prompt certain 3P-ASPs to prefer working through PDGs than directly with individuals. Imagine, for example, a 3P-ASP who is a university researcher and who seeks a better understanding of daily commuting practices in the County of Los Angeles in order to combat air pollution. This 3P-ASP needs to access not only one Personal Data Stream, but hundreds of thousands. But if all these data are locked away in separate PDVs, a researcher cannot easily access them—

[112] Protection of Human Subjects, 45 C.F.R. § 46 (2010).

[113] *See* H. Tristram Engelhart, Jr., *Basic Ethical Principles in the Conduct of Biomedical and Behavioral Research Involving Human Subjects, in* NAT'L COMM'N FOR THE PROT. OF HUMAN SUBJECTS OF BIOMEDICAL & BEHAVIORAL RESEARCH, THE BELMONT REPORT 7-39, 8-5 to -6 (1979) (defining basic principles for research ethics).

unless PDGs answer federated queries.[114] In other words, we can think of individual PDVs connecting together to form a sort of Personal Data Cloud. One could envision the creation of communication protocols and standards that enable PDGs to collaborate in answering aggregate queries made by service providers, such as our hypothetical researcher.

We are cautious about this possibility because a massive Personal Data Cloud that can be accessed by third parties seems to be antithetical to increasing privacy. Our assumption is that PDGs, motivated by their role ideology and constrained by the law, will help individuals make informed decisions in the individuals' best interest that could include sometimes sharing information in order to further the public good. As already explained, there are benefits to society from self-surveillance, and the PDG seems to be the most effective way to tease them out without sacrificing the individual's privacy.

B. USELESS?

1. Third-Party Surveillance

A second major objection is that a PDG is useless because self-surveillance is not the real problem. Instead, the real threat is third-party surveillance of us. Above, we noted that self-surveillance should be distinguished from the harder problem of third-party surveillance of us.[115] Although that distinction is crucial, one could object that third-party surveillance of us is now so pervasive and detailed that the contents of a PDV would not be unique.[116]

Take, for example, the CENS Participatory Sensing case study. The core of the Personal Data Stream is location data captured by a GPS sensor voluntarily worn by the individual. But location can be determined fairly accurately through mobile-phone triangulation techniques. And soon, even commodity phones will have GPS radios built in. Since location information is then available to a mobile-phone provider, such as Verizon, perhaps the provider's surveillance can produce the same data that self-surveillance would.

[114] This is similar to an approach suggested by the Common Data Project, a nonprofit organization developing a cloud service that would allow third parties to query sensitive personal data without revealing that data. THE COMMON DATA PROJECT, WHITE PAPER V.2 13–31 (2011), *available at* http://www.commondataproject.org/docs/whitepaper.pdf.

[115] *See supra* Part III.C.1.

[116] Here are some other examples. Suppose that instead of getting an individual to spit carefully five milliliters into a sterile test tube, one could get her DNA simply by shaking her hand or collecting the wine glass she has drunk out of. Suppose that in the near future, instead of placing a software bug that records how we work on our computers, everything—browsing, email, calendaring, games—is done through Microsoft or Google or the wireless broadband service provider, who then collects all the information directly.

On the one hand, this objection carries much force. If it is true that third parties can collect as much telling data as self-surveillance, then the PDG solution is partial at best, pointless at worst. On the other hand, we have good reason to believe that self-surveillance collects qualitatively more sensitive data than does third-party surveillance. First, as a technological matter, self-surveillance currently can produce much more telling data than third-party surveillance. Perhaps that gap will narrow as better surveilling technologies go mainstream, but some such gap will likely persist into the foreseeable future.[117] Second, as a political matter, many such technologies deployed by third parties will be constrained since they will be deemed politically and socially unacceptable. Thus, even if technology could eliminate that gap, laws and social norms will likely keep that from happening. In the meantime, the problem and possibility of self-surveillance privacy remains to be solved.

2. Genie Out of the Bottle

Even if an entire profession of PDGs comes online, 3P-ASPs will likely gain some access to the self-surveillance data in order to provide the most useful and sophisticated analysis. This is notwithstanding commitment to the parsimony principle. But this raises the perennial privacy question of what to do with secondary data transfers. Once the data leave the PDV, won't the data in practice lose all protections? This is the genie-out-of-the-bottle problem.

This is a serious and difficult problem, which we did not create and is hardly unique to our proposal. In fact, the "genie" problem is much worse when third parties, who are less constrained in their secondary transfers, store personal data directly. By contrast, our PDG approach makes real improvements. Most important is that the PDG seeks to constrain secondary transfers that risk decreasing privacy. Besides advising her clients accordingly, a PDG can pursue certain technological and legal strategies to mitigate the genie-out-of-the-bottle problem.

a. Self-Help Lockdown

A technological strategy would be to wrap personal data in Privacy Rights Management ("PRM") that increases the likelihood that the personal data will be processed only in authorized ways. Similar to the Digital Rights Management ("DRM") system that copyright holders deploy, PRM could use audit trails[118] to revoke access to user data in the case of a violation. Services

[117] Consider second- and third-generation iterations: What if the vault encourages third-party surveillers to deposit their data on you into your PDV. This would include your bank, your mobile-phone provider, your cable company, your local government, and your health record, for example. All their data on you would be deposited into your account!

[118] *See infra* Part V.B.2.b (discussing TraceAudits).

such as Ephemerizer[119] and Vanish[120] provide plausible examples. It is also possible to imagine that users could take back data if they changed their minds about the consequences of data sharing ("remote revocation").

b. Contractual Transitivity

A legal strategy would be to embed a sort of contractual transitivity of obligations that flow with the personal data to 3P-ASPs. In other words, before any PDG would allow a 3P-ASP to access, possess, or process personal data, it must itself enter into a contract that includes promises by the 3P-ASP to respect the various obligations (confidentiality, care, etc.) that the PDG has to the client. Moreover, this contract could explicitly list the client as an intended third-party beneficiary,[121] with the right to sue the 3P-ASP for breach of its contract with the PDG.[122]

[119] *See* RADIA PERLMAN, THE EPHEMERIZER: MAKING DATA DISAPPEAR (Sun Microsystems Labs., Technical Report No. TR-2005-140, 2005), *available at* labs.oracle.com/techrep/2005/smli_tr-2005-140.pdf.

[120] *Vanish: Self-Destructing Digital Data*, UNIV. OF WASH., http://vanish.cs.washington.edu (last visited Jan. 22, 2012).

[121] *See* RESTATEMENT (SECOND) OF CONTRACTS § 302 (1981). Even without an express designation, in most jurisdictions, intended-beneficiary status might still be found when the circumstances suggest that the party to the contract that extracted the promise (the Guardian) did so for the benefit of the third party (the client). *See id.* § 304 cmt. e (suggesting that courts look to whether "recognition of the right will further the legitimate expectations of the promisee, make available a simple and convenient procedure for enforcement, or protect the beneficiary in his reasonable reliance on the promise").

But some jurisdictions, such as New York, resist looking beyond the four corners of the contract. *See, e.g.*, Debary v. Harrah's Operating Co., 465 F. Supp. 2d 250, 263 (S.D.N.Y. 2006) (citing Newman & Schwartz v. Asplundh Tree Expert Co., 102 F.3d 660 (2d Cir. 1996)), *aff'd sub nom.* Catskill Dev., L.L.C. v. Park Place Entm't Corp., 547 F.3d 115 (2d Cir. 2008). To satisfy these jurisdictions and to avoid the uncertainty that inherently accompanies a judicial determination of intended-beneficiary status, explicit identification of the client as an intended beneficiary in the contract itself makes sense.

[122] Courts routinely recognize the right of an intended third-party beneficiary of a contract to recover damages for breach. *See, e.g.*, Cnty. of Santa Clara v. Astra USA, Inc., 540 F.3d 1094, 1109 (9th Cir. 2008) (finding that local medical clinics are intended third-party beneficiaries that may recover damages from pharmaceutical companies resulting from the alleged breach of pricing agreements with the federal government), *opinion withdrawn and superseded*, 588 F.3d 1237 (9th Cir. 2009), *rev'd*, 131 S. Ct. 1342 (2011) (holding that healthcare facilities cannot sue pharmaceutical manufacturers as third-party beneficiaries to enforce pricing agreements between the federal government and the manufacturers because such suits are incompatible with the statutory scheme); Colavito v. N.Y. Organ Donor Network, Inc., 438 F.3d 214 (2d Cir. 2006) (holding that a prospective kidney donee who sued a donor network and others when a kidney that was donated on the condition that he receive it was implanted in another person was an intended third-party beneficiary), *certified question answered*, 860 N.E.2d 713 (N.Y. 2006) (holding that the intended donee had no common-law right to an incompatible kidney and, thus, no cause of action for conversion, and that the intended donee also had no right of action under New York's Public Health Law for an incompatible kidney); Vanerian v. Charles L. Pugh Co., 761 N.W.2d 108, 109, 114 (Mich. Ct. App. 2008) (holding that a homeowner was an intended third-party beneficiary of a contract between a

This strategy runs into at least two problems: one practical, the other legal. The practical problem is detecting 3P-ASPs contract violations. A "TraceAudit" could help. The TraceAudit is a log included in the PDV that is meant to increase the visibility of outside access and use of vault data. The TraceAudit requires that third-party applications log all activities performed on or with user data. This log is maintained by the PDG and can be viewed by her clients who may be curious about how their data have been used. It can also be used to detect suspicious events[123] or alert users to possible violations of data-use policy.

The legal problem is that even when a violation is detected, what relief would be granted when damages are hard to calculate? Contract damages are typically limited to unavoidable, certain, and foreseeable economic losses.[124] Unless and until a robust market for self-surveillance data develops (something we are not eager to see), the violation of contractually transferred obligations would not create any of the standard economic losses for which courts routinely provide compensation.[125] Instead, damages due to breach of privacy terms are more properly considered emotional or psychic losses, forms of harm that courts generally do not recognize as contractual damages unless "the contract or the breach is of such a kind that serious emotional disturbance was a particularly likely result."[126] For certain types of Personal Data Streams, this standard may well be met, and the very fact that the data were stored with the PDG could help signal that serious emotional disturbance is likely.[127]

subcontractor and a general contractor to install a floor in her home). By contrast, incidental beneficiaries have no legal recourse in the event of a breach.

[123] "[Fraud-detection] systems employ some machine learning and statistical analysis algorithms to produce *pattern-directed inference systems* using models of anomalous or errant transaction behaviors to forewarn of impending threats." Salvatore J. Stolfo et al., Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results 1 (unpublished manuscript), http://wenke.gtisc.gatech.edu/papers/credit_card_FD.ps (last visited Jan. 22, 2012). For an additional description of fraud-detection systems, see Richard J. Bolton & David J. Hand, *Statistical Fraud Detection: A Review*, 17 STAT. SCI. 235 (2002).

[124] RESTATEMENT (SECOND) OF CONTRACTS §§ 347, 351–52 (1981).

[125] *See In re* Jetblue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 326–27 (E.D.N.Y. 2005).

[126] RESTATEMENT (SECOND) OF CONTRACTS § 353.

[127] Whether violation of contracts guaranteeing privacy allow for damages for emotional distress has seemingly turned on the nature of information that was improperly disclosed. *Compare* Trikas v. Universal Card Servs. Corp., 351 F. Supp. 2d 37, 46 (E.D.N.Y. 2005) (awarding no damages for improper disclosure of credit report), *with* Huskey v. Nat'l Broad. Co., 632 F. Supp. 1282, 1293 (N.D. Ill. 1986) (allowing a prisoner to recover damages for defendant's improper national broadcast of images of him incarcerated). If we assume that this is ultimately grounded in the principles of foreseeability of particular harm by the contracting parties enshrined in *Hadley v. Baxendale*, (1854) 156 Eng. Rep. 145 (Exch. Div. 1854), then the existence of a PDG and the act of stipulating damages itself would seem to alert both parties to the harm and to allow for recovery of damages.

To avoid such complications, the best practice would be for PDGs to include liquidated-damage clauses.[128] Courts will only enforce provisions that are "reasonable in the light of the anticipated or actual loss caused by the breach."[129] The harder it is to determine actual damages, the more latitude courts will grant to those stipulated by the parties.[130] Because the precise level of these damages is difficult, if not impossible, to quantify, a conservative stipulation of psychic losses should pass judicial scrutiny. The possible threat of class-action aggregation of small claims would increase the enforcement stakes.

VI. CONCLUSION

In privacy debates, any new problem is often met by calls for direct regulation or laissez faire trust of the market. Our approach seeks a novel path between the two. Instead of direct behavioral regulation or blind faith in the market, our strategy is to modify indirectly the information ecosystem by introducing a new species, the PDG. This new creature would be a faithful agent to its client and would store self-surveillance data in its PDV. The PDG would also act as a professional intermediary with third parties who seek access to such data.

Although we have painted with broad strokes, we believe that the PDG framework is a viable, concrete solution to the problem of self-surveillance. What is more, if the PDGs come to be, they will themselves become invested stakeholders, able to shape and alter future privacy policies in this and other domains. Indeed, if the framework functions well in this context, it could be expanded incrementally to help solve adjacent or related privacy problems.[131]

Novel solutions to privacy problems have become scarce. Simple inspection of the privacy landscape demonstrates that industry self-regulation, self-help encryption, and formalistic notice-and-consent clickwraps are not up to the task. The time for the PDG is at hand.

[128] *See, e.g.*, EEOC v. First Citizens Bank of Billings, 758 F.2d 397, 403 (9th Cir. 1985) ("Liquidated damages are compensatory, not punitive in nature."); United States v. Am. Motorists Ins. Co., 680 F. Supp. 1569, 1572 (Ct. Int'l Trade 1987) ("True liquidated damages are not penalties. They are compensatory in nature, providing a measure of recovery when it appears at the time a contract is made that damages caused by breach will be difficult or impossible to estimate.").

[129] RESTATEMENT (SECOND) OF CONTRACTS § 356.

[130] *Id.* § 356 cmt. b.

[131] Two such problems could include medical data, even if it falls outside our current definition of self-surveillance data, and user authentication across the Internet.

THE UNIVERSITY OF IOWA
ORGANIZED FEB. 25TH 1847.