2012

Privacy & the Personal Prospectus: Should We Introduce Privacy Agents or Regulate Privacy Intermediaries

Scott R. Peppet
University of Colorado Law School

Privacy & the Personal Prospectus: Should We Introduce Privacy Agents or Regulate Privacy Intermediaries?

Scott R. Peppet[*]

* Professor of Law, University of Colorado School of Law.

INTRODUCTION

Kang et al.'s *Self-Surveillance Privacy*[1] ("*SSP* ") is timely, important, and correct: self-surveillance is both increasing and a potential threat to privacy. In this brief response essay I first highlight the significant contributions in *SSP*, particularly the novel conception of "flow" as a privacy metric and the focus throughout on the growing phenomenon of self-surveillance. I tie *SSP*'s idea of the "data vault" to what I have elsewhere labeled the "personal prospectus"[2] and agree that self-aggregated information is an increasingly important privacy concern.

At the same time, I raise three complications. First, although *SSP* tries to distinguish self-surveillance technologies from third-party-privacy problems,[3] I argue that the distinction is unlikely to be so clean in practice. Self-surveillance technologies are generally consumer products encumbered by contractual arrangements that give their makers access to the data those products generate. Although *SSP* relies on the first-party/third-party distinction to assert that in self-surveillance only the individual user has a claim to ownership of the underlying data, in many consumer contexts this is not the case. Particularly when a hardware product is sold at a discount or a loss to drive users into profitable long-term service agreements, *SSP*'s distinction seems inadequate.[4]

Second, even assuming that one could implement the *SSP* proposal and sequester self-surveillance data in a secure, privileged data vault, there would still be pressure on consumers to release the data into the economy. This is the unraveling problem for privacy—that giving a consumer control over her data is not necessarily sufficient to prevent the consumer from feeling forced to reveal that data.[5]

Given these concerns, this response essay ends with a question: rather than introducing privacy agents, should we perhaps instead regulate firms that deal in self-surveillance data as privacy intermediaries?[6] We may be stuck with an architecture in which firms collect self-surveillance data for consumers and use the data in various ways, including in marketing or other transactions that may or may not always be in the consumer's best interest. How should such firms be regulated to protect consumers? This may, ultimately, be the route we must take, despite the fact that it is—as *SSP* acknowledges—a harder nut to crack.

---

1. Jerry Kang et al., *Self-Surveillance Privacy*, 97 IOWA L. REV. 809 (2012).

2. *See* Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U. L. REV. 1153, 1166 (2011) (explaining the personal prospectus).

3. *See* Kang et al., *supra* note 1, at 825–26.

4. *See infra* Part II.A.

5. *See infra* Part II.B.

6. *See infra* Part II.C.

Before we start, one caveat. Because of the very short format of this response, I have avoided describing *SSP*'s argument except where absolutely necessary; I assume the reader is familiar. Similarly, I make no attempt here to review comprehensively each aspect of the essay. Instead, I focus on a few interesting bits and raise questions and concerns to provoke further discussion of this valuable addition to the privacy literature.

I. YES . . .

A. *SELF-MEASUREMENT & THE INCREASING IMPORTANCE OF THE PERSONAL PROSPECTUS*

SSP makes one assertion about which there should be no debate: human instrumentation is booming. A Fitbit monitor can track the number of steps you take in a day, how many miles you've walked, calories burned, and how many minutes you have slept.[7] BodyMedia's armbands[8] are similar, as is the Philips DirectLife device[9] and the Nike Fuel Band.[10] You can track your running habits with RunKeeper,[11] your weight and body fat with a WiFi-enabled scale,[12] your blood pressure with a wireless blood pressure monitor,[13] or your emotional arousal with an Affectiva Q Sensor.[14] You can monitor your sleep with a Zeo[15] or SleepTracker device,[16] your pulse and temperature with a Basis sports watch,[17] your heart rate with your iPhone and a Bluetooth-enabled Wahoo heart rate monitor,[18] your diabetes management with the iBGStar iPhone add-on and app,[19] your alcohol intake

7. *See Fitbit Ultra Overview*, FITBIT, http://www.fitbit.com/product (last visited July 8, 2012).

8. *See What Is BodyMedia FIT?*, BODYMEDIA, http://www.bodymedia.com/Products/Learn-More/What-is-BodyMedia-FIT (last visited July 8, 2012).

9. *See DirectLife*, PHILIPS DIRECTLIFE, http://www.directlife.philips.com (last visited July 8, 2012).

10. *See Nike+ Fuelband*, NIKE, http://www.nike.com/fuelband (last visited July 8, 2012).

11. *See* RUNKEEPER, http://www.runkeeper.com (last visited July 8, 2012).

12. *See Fitbit Aria Overview*, FITBIT, http://www.fitbit.com/product/aria (last visited July 8, 2012); *The Intelligent Scale*, WITHINGS, http://www.withings.com/en/bodyscale (last visited July 8, 2012).

13. *See* IHEALTH, http://www.ihealth99.com/BP3_feature.html (last visited July 28, 2012); *Blood Pressure Monitor*, WITHINGS, http://www.withings.com/en/bloodpressuremonitor (last visited July 8, 2012).

14. *See Q Sensor*, AFFECTIVA, http://www.affectiva.com/q-sensor (last visited July 8, 2012).

15. *See* ZEO, http://www.myzeo.com/sleep (last visited July 8, 2012).

16. *See* SLEEPTRACKER, http://www.sleeptracker.com (last visited July 8, 2012).

17. *See Basis Product Tour*, BASIS, http://www.mybasis.com/product/#/tech (last visited July 8, 2012).

18. *See* WAHOO FITNESS, http://www.wahoofitness.com (last visited July 8, 2012).

19. *See The iBGStar Diabetes Manager Application*, IBGSTAR, http://www.ibgstar.us/iphone-app.aspx (last visited July 8, 2012).

with Drinking Diary,[20] your jogging with Smashrun,[21] your sexual history with BedPost,[22] your driving habits with CarChip,[23] your energy use with Wattvision,[24] the music you listen to with Last.fm,[25] and your movements and location with WhereDoYouGo,[26] Trackr!,[27] or Placeme.[28] Beyond merely recording your behavior, these technologies also seek to change it: you can motivate yourself to exercise more, for example, by carrying a Striiv device[29] in your pocket that rewards your exertions with electronic badges and prizes.

Some call this physiological computing,[30] personal informatics,[31] or the "quantified self" movement.[32] In what I call "Generation One" of this trend, enthusiasts have hacked together hardware and software innovations to collect and analyze data about all facets of daily life. An inventor in England named Dale Lane, for example, recently used a personal computer to track his television viewing habits so that he could analyze what he and his family watched, when, for how long, and how often.[33] He then added a web-enabled camera that photographed him as he watched television. Combined with free facial-analysis software from the web service Face.com, this allowed Lane to analyze how often he smiled while watching a particular television program, revealing in minute detail his likes and dislikes.[34] Similarly, a computer scientist named Stephen Wolfram recently published an analysis of over twenty years of self-collected data documenting his phone call and email habits—data he had collected using various devices and systems he created.[35]

---

20. *See* DRINKINGDIARY.COM, http://www.drinkingdiary.com/index.html (last visited July 8, 2012).

21. *See* SMASHRUN, http://www.smashrun.com (last visited July 8, 2012).

22. *See* BEDPOST, http://www.bedposted.com (last visited July 8, 2012).

23. *See CarChip Pro*, CARCHIP, http://www.carchip.com/Products/8226.asp (last visited July 8, 2012).

24. *See* WATTVISION, http://www.wattvision.com (last visited July 8, 2012).

25. *See* LAST.FM, http://www.last.fm (last visited July 8, 2012).

26. *See* WHERE DO YOU GO, http://www.wheredoyougo.net (last visited July 8, 2012).

27. *See* TRACKR!, http://www.trackr.eu (last visited July 8, 2012).

28. *See* PLACEME, http://www.placemeapp.com/placeme/index.html (last visited July 8, 2012).

29. *See* STRIIV, http://www.striiv.com (last visited July 8, 2012).

30. *See Physiological Computing: Where Brain and Body Drive Technology*, PHYSIOLOGICAL COMPUTING, http://www.physiologicalcomputing.net (last visited July 8, 2012).

31. *See Know Thyself*, PERSONAL INFORMATICS, http://personalinformatics.org (last visited July 8, 2012).

32. *See Quantified Self: Self Knowledge Through Numbers*, QUANTIFIED SELF, http://quantifiedself.com (last visited July 8, 2012).

33. *See* Dale Lane, *What Do I Watch on TV?*, DALELANE.CO.UK, http://dalelane.co.uk/tvscrobbling (last visited July 8, 2012).

34. *See* Dale Lane, *Smile!*, DALELANE.CO.UK (Apr. 3, 2012, 10:29 PM), http://dalelane.co.uk/blog/?p=2092.

35. *See* Stephen Wolfram, *The Personal Analytics of My Life*, STEPHEN WOLFRAM BLOG (Mar. 8, 2012), http://blog.stephenwolfram.com/2012/03/the-personal-analytics-of-my-life.

Such data analysis is increasingly available to consumers not interested in writing their own code or hacking their own hardware together. This is "Generation Two" of the self-surveillance movement—the commercialization of self-tracking and self-surveillance sensor devices. Web services such as Baby Connect, Total Baby, Baby Log, and Trixie Tracker, for example, allow thousands of parents to record the sleep, eating, and digestive habits of their newborns: since Baby Connect launched in 2009, its users have input over 47 million such "events."[36] New hardware products are under development to relieve users of the need to do such input manually.[37] Although very little research exists on the prevalence of self-tracking using Generation Two consumer products, one early study suggests that approximately one-quarter of internet users have tracked some aspect of their health online.[38]

SSP is right to call attention to these new streams of personal data. Sensors are becoming far less expensive and far more common. Consider just today's smartphones, which now contain a compass (to detect physical orientation), accelerometer (to track the phone's movement in space), ambient light monitor (to adjust screen brightness), proximity sensor (to detect whether the phone is near your face), and gyroscope (to detect the phone's orientation vertically or horizontally), as well as GPS, a sensitive microphone, and multiple cameras. Research is underway to further enhance smartphones to detect ultraviolet radiation levels (to help prevent skin cancer),[39] pollution levels (to help monitor one's environment),[40] and various indicators of health, activity, and well-being,[41] including sensors that can monitor blood alcohol levels and body fat.[42]

---

36. *See* Mya Frazier, *The Data-Driven Parent*, ATLANTIC, May 2012, at 28, *available at* http://www.theatlantic.com/magazine/archive/2012/05/the-data-driven-parent/8935.

37. Evoz and Belkin, for example, are developing a Wi-Fi enabled monitoring device. *See Belkin and Evoz Join Forces To Create Wi-Fi Enabled Baby Monitoring Solutions*, REUTERS.COM (Jan. 3, 2012, 1:59 PM), http://www.reuters.com/article/2012/01/03/idUS150850+03-Jan-2012+BW20120103.

38. *See* SUSANNAH FOX, PEW RESEARCH CTR., THE SOCIAL LIFE OF HEALTH INFORMATION, 2011 (2011), *available at* http://www.pewinternet.org/~/media//Files/Reports/2011/PIP_Social_Life_of_Health_Info.pdf.

39. *See New Sensors for Smartphones*, MIT MOBILE EXPERIENCE LABORATORY, http://mobile.mit.edu/research/new-sensors-smartphones (last visited July 8, 2012).

40. *See* DAVID HASENFRATZ ET AL., COMPUTER ENGINEERING AND NETWORKS LABORATORY, PARTICIPATORY AIR POLLUTION MONITORING USING SMARTPHONES 1 (2012), *available at* ftp://www.tik.ee.ethz.ch/pub/people/hdavid/HSST2012.pdf.

41. *See, e.g.*, Sean T. Doherty & Paul Oh, *A Multi-Sensor Monitoring System of Human Physiology and Daily Activities*, 18 TELEMEDICINE & E-HEALTH 185, 185–86 (2012) (using smartphone along with an electrocardiogram and a blood-glucose monitor to track health and activity).

42. *See* Andrew Ku, *Smartphones Spotted with Breathalyzer, Body Fat Sensors*, TOM'S HARDWARE (Mar. 2, 2012, 6:00 AM), http://www.tomshardware.com/news/NTTidocomo-smartphone-breathalyzer-weather-health,14863.html.

I have elsewhere focused on such sensor data, arguing that they offer both the promise of self-revelation and various kinds of privacy perils.[43] In particular, I have introduced the notion that over time each of us increasingly will have a "personal prospectus"—a compilation of an individual's verified private information about himself or herself.[44] The personal prospectus will contain information obtained through digital monitoring of directly observable data—this is the self-surveillance sensor data on which *SSP* focuses. In addition, the personal prospectus may also contain directly verifiable data—such as financial, educational, or criminal records—that is accumulated in one location in verified form.[45] *SSP* does not focus on this second type of information, but it is as important as directly observable sensor data. All of this information can and will be useful to individuals as they attempt to assert themselves in the economy by signaling their qualities to other economic actors.[46]

At the most basic level, then, *SSP* deserves recognition for helping to draw attention to this trend and to the privacy implications of sensor-based self-surveillance data. Sensors and other monitoring devices are likely to have far-reaching legal implications, beyond just the privacy domain, that deserve consideration by the academic and policy communities. In the criminal context, for example, will self-surveillance data (e.g., constant location tracking via a smartphone's GPS records) become a standard alibi or be used (e.g., pulse or other biometric data that tracks emotional or physical arousal or stress) to establish mens rea? In the family law context, will monitoring one's child via such sensors become expected and part of the baseline standard of care? In the employment and healthcare contexts, will employers be able to seek access to self-surveillance data (e.g., caloric intake, exercise habits, sleep patterns) for insurance purposes or as part of a corporate wellness program? These questions deserve study, and *SSP* makes a contribution by highlighting the rise of sensor-driven monitoring.

B. FLOW

In addition, *SSP* tantalizes with a brief discussion of a novel conception of privacy based on the relative "flow" of information through an information context. The standard conception of privacy as control over one's information has various shortcomings, which have been well thrashed out.[47] Nevertheless, many discussions of privacy ultimately return to control-

43. *See* Peppet, *supra* note 2, at 1167–73; Scott Peppet, *The Quantified Self: Personal Choice and Privacy Problem?*, CONCURRING OPINIONS (Nov. 16, 2010, 6:28 PM), http://www.concurringopinions.com/archives/2010/11/the-quantified-self-personal-choice-and-privacy-problem.html.

44. *See* Peppet, *supra* note 2, at 1166–67.

45. *Id.* at 1173–76.

46. *Id.* at 1176–82.

47. *Id.* at 1186 n.158 (citing literature that is critical of privacy as control).

based conceptions.[48] Flow seems, at first blush, to offer a different metric that could move the conversation beyond control. *SSP*'s authors plant a "scholarly flag" indicating a desire to return to these questions.[49] I urge them to do so quickly.

When they do, I hope they will explore how conceiving of privacy in terms of information flow settles or solves existing privacy problems or debates in the informational privacy literature. In short, to what questions is flow an answer? I can offer one: I have recently drawn attention to the problem that "voluntary" sharing of one's information can sometimes present a privacy issue,[50] particularly in contexts in which individuals feel pressured to reveal their private information because others have done so and a social or economic stigma will attach if they stay quiet.[51] Control conceptions of privacy do not properly account for this type of problem: the orthodox response from such a point of view is that voluntary self-disclosure presents no privacy issues so long as the consent is valid. Flow, however, seems to fit well as an explanation for why in some contexts voluntary disclosure may still be privacy-depleting or invasive. As Kang et al. mention, "according to our flow conception, it doesn't matter that an individual consents."[52] The flow metric may thus provide a useful means for talking about privacy problems in the context of "forced disclosure" or the unraveling of privacy.

Similarly, *SSP*'s authors may be able to connect their idea of flow to Harry Surden's work on "structural privacy"—the ways in which certain types of information have remained functionally private because they have historically been difficult to gather, analyze, and store even if they were technically public.[53] Court records might have always been available in the dusty file cabinets of a county courthouse, but does this completely eliminate any privacy issue once those records are digitized and made available on the internet? Our traditional conceptions of privacy as control suggest that there is no privacy problem with such frictionless access, given that the information was always available in some form in the public domain. But flow suggests otherwise: the harm, to the extent there is one, can be measured by the increase in movement of these data into and across information contexts in new ways. Again, flow may prove a useful means for understanding certain privacy problems that have sometimes been difficult

48. *Id.* at 1185–90 (discussing the ways in which control continues to pervade privacy literature).

49. *See* Kang et al., *supra* note 1, at 822 ("[W]e mean to plant a scholarly flag to mark further inquiry.").

50. *See* Peppet, *supra* note 2, at 1183–90.

51. *See infra* Part II.B.

52. Kang et al., *supra* note 1, at 822 n.33.

53. *See* Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605, 1613–15 (2007).

to grapple with in its absence. There are undoubtedly many other points of contact to explore;[54] I will leave those for *SSP*'s authors.

C. Privacy Agents, Privacy Vaults & Privacy Privilege

Finally, *SSP* should be applauded for its focus on a structural solution to privacy problems—changing the players, and type of players, in the mix. Specifically, *SSP*'s introduction of a new type of professional privacy agent—the personal data "guardian"—is a wise attempt to reengineer the problem of self-surveillance data rather than merely argue within the constraints of the existing structure of that problem (e.g., about whether consumers are sufficiently informed by privacy policies, etc.).

SSP's focus on privacy-enhancing agents is noteworthy for advocating for a new type of professional—a human being with legal obligations. Much of the early computer science work on internet privacy focused on the use of automated software "agents," or what Lawrence Lessig early on called the "electronic butler."[55] The core idea of such software agents was that they would learn a user's privacy preferences and then automatically negotiate with websites that the user visited to ensure that the sites met the user's privacy requirements.[56] *SSP* argues for a very different approach: state licensing of privacy agents charged with protecting their clients' data (by securing it in privacy "vaults") and privacy preferences (by negotiating on their clients' behalves with vendors and others interested in such data).[57]

All of this is laudable, although Part II raises some doubts about the efficacy of such privacy agents.[58] It is important, however, to distinguish these two concepts—privacy agents and privacy vaults—and not to assume that one is inextricably tied to the other. In particular, it is very helpful that *SSP* focuses on privacy vaults and begins to explicate the function they could serve. I have elsewhere argued for a similar concept, particularly the notion that data can be processed within a privacy vault without revealing the

---

54. Another may be Julie Cohen's work on "semantic discontinuity" or the need for "gaps" in the semantic web so that individuals have some space in which to live. *See* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 223–66 (2012). Such gaps seem similar, in some ways, to conceiving of privacy in terms of slowing down the flow of information. I thank Paul Ohm for this connection.

55. *See* LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE 160 (1999).

56. *See* Daniel Le Métayer & Shara Monteleone, *Automated Consent Through Privacy Agents: Legal Requirements and Technical Architecture*, 25 COMPUTER L. & SECURITY REV. 136, 140 (2009) ("[A] Privacy Agent can be defined as a software system offering two essential functionalities: (1) a User Interface dedicated to the interactions with the subject (for example to allow him to define his 'privacy policy') and (2) a Data Manager controlling the disclosure of personal data.").

57. *See* Kang et al., *supra* note 1, at 828–31.

58. *See infra* Part II.A.

ownership of those data.[59] From a technical standpoint, privacy vaults make great sense.

Privacy vaults need not, however, be administered by privacy agents with fiduciary obligations to one client (the individual data owner). Instead, privacy vaults might be more like trusts—administered by a trustee with fiduciary obligations to multiple parties.[60] Or we may need to define a set of legal obligations for "privacy intermediaries" that run such vaults—entities that are clearly serving as middlemen, but in a regulated system like other intermediaries in the economy. One might want Google and Facebook, for example, to have certain obligations of competence and confidentiality, but these entities are clearly not "agents" in the sense in which *SSP* means. The point here is that each idea—privacy agents and privacy vaults—may have merit, and they may indeed have merit in combination. But they should also be fully considered in alternative configurations separate from each other. We will return to this discussion below.[61]

Finally, *SSP*'s focus on the possibility of privileging sensitive information to fend off a future subpoena is important and also contributes a promising tool to the privacy literature.[62] It should also, however, be separated from the article's focus on personal data guardians and personal data vaults. If consumers would not use self-surveillance technologies in socially optimal ways without privilege, it might attach not only to information held in a personal data vault but to any sensor-collected information, even if secured elsewhere. Indeed, it is difficult to see why self-surveillance data should be the only information protected through such a privilege, if indeed such privileges are necessary. Why not search queries, smart phone location data, or other sensitive digital information? *SSP* tantalizes by offering this limited privilege, but the argument for legally fencing off self-surveillance information—while leaving so many other types of personal information unprotected—deserves further discussion. Until that point, we should consider the potential of privileging all such information, whether or not that protection is tied to a personal data guardian or personal data vault.

II. BUT . . .

Having celebrated some of the most foundational aspects of *SSP*, let us turn to a few questions or doubts. I raise three: (1) how to address the commercial reality that much self-surveillance will take place using

---

59. *See* Scott R. Peppet, *Smart Mortgages, Privacy and the Regulatory Possibility of Infomediation* (U. Colo. Law: Legal Studies Research Paper Series, Working Paper No. 09–13, 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1458064.

60. *See id.* at 53–56 (discussing how a privacy intermediary might be best analogized to the trustee model).

61. *See infra* Part II.C.

62. *See* Kang et al., *supra* note 1, at 832–36 (discussing the potential evidentiary privilege that could be granted to self-surveillance data).

consumer products that come with contractual complications that may undermine the personal data guardian idea; (2) how to address the unraveling problem that self-surveillance data create; and (3) whether it would be more effective to more heavily regulate existing "privacy intermediaries" than to try to introduce a new species of privacy agents.

A. *Is This Really a Third Party Surveillance Problem After All?*

SSP distinguishes self-surveillance—in which an individual has control over sensors and other devices that record data—from third-party surveillance problems—in which a counterparty such as a merchant or device manufacturer "collects the personal data in the course of interacting . . . with the individual."[63] As *SSP* puts it:

> With self-surveillance . . . the counterparty's interest disappears because the counterparty does not exist . . . . Rather, these data are created by purposeful, self-initiated surveillance through sensors within the individual's control . . . . Accordingly, no counterparty . . . has proprietary claim to such data; it didn't collect the data in the first place and often couldn't . . . even if it wanted to.[64]

This is a critical distinction that underlies the rest of *SSP*'s argument, because *SSP* assumes for the remainder of the article that an individual *can* sequester her information in a data vault through a personal data guardian because the individual is the only party with rights to or interests in those data.

In an academic research context—such as the Participatory Sensing example discussed in *SSP*[65]—this lack of a third party might be descriptively accurate. Similarly, an individual innovator or ambitious hobbyist might be able to jerry-rig simple sensors and code the software needed to collect and analyze the data produced by those devices. In such Generation One self-surveillance scenarios, the individual truly is engaged in "pure" self-surveillance without the involvement of third parties. Both Dale Lane and Stephen Wolfram, for example, clearly had the technical skills to assemble their own hardware and software to record and analyze their self-surveillance data.[66]

In the many Generation Two consumer examples already discussed—such as Fitbit, DirectLife, BodyMedia, Nike's FuelBand or Striiv[67]—this is not, however, the case. Instead, a firm produces a hardware sensor that a consumer purchases and uses subject to various terms and conditions. In addition, these hardware components are often tied to the firm's web site or

---

63. Kang et al., *supra* note 1, at 825.
64. *Id.* at 826.
65. *Id.* at 815–17.
66. *See supra* notes 33–35 and accompanying text.
67. *See supra* notes 7–10, 29 and accompanying text.

service for aggregating and analyzing the sensor data. A Fitbit user, for example, can log on to Fitbit.com to see charts and graphs of her data in action. This is the trajectory of self-surveillance at commercial scale, and it provides manufacturers of such devices with an intimate portrait of their users. Somewhat paradoxically, *SSP* is still correct to label such activity "self-surveillance," because self-measurement does differ from the surreptitious third-party tracking that is the focus of much internet privacy literature. At the same time, "pure" self-surveillance without *any* involvement of third-party firms is rare.

In a footnote, *SSP* acknowledges that the distinction between self-surveillance and third-party surveillance may not hold completely:

> 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 distinction[] . . . which presumed that no such assistance was needed. We concede that contracting away rights to data can always complicate the picture.[68]

Unfortunately, this concession seems far more important than a footnote implies. The academic research context or isolated Generation One hobbyist who can hack her own hardware and software together are not the examples that matter. The fundamental question is how self-surveillance will scale—or, more accurately, is scaling—to become widely accessible to consumers rather than hobbyists. What business models will firms adopt to support these sensor technologies and data analysis services? How are these products being developed, marketed, and sold, and does that complicate *SSP*'s idea of introducing Personal Data Guardians to serve as privacy agents?

I believe it does. Consider just a few examples of existing consumer self-surveillance products. In a sense, hardware manufacturers like Fitbit and Zeo seem to be merely selling a self-surveillance device. One could imagine such devices working with *SSP*'s data guardian structure, because an individual user could theoretically choose to re-route his or her Fitbit or other data from the device to the data guardian.

In reality, however, the legal relations and economics of consumer self-surveillance are more complex. Many existing consumer self-surveillance products are not one-shot purchases in which the consumer buys a device that the consumer then controls completely. Instead, the purchase of the device itself is merely the beginning of a long-term service arrangement between the consumer and the manufacturer, who hopes to provide data

68. Kang et al., *supra* note 1, at 826 n.53.

storage and analysis services to the user. Thus, the popular Fitbit exercise monitor, for example, costs $99.95 to purchase but an additional $49.99 per year for "Fitbit Premium" data services.[69] The device synchronizes almost automatically with Fitbit's web services once taken out of the box, and without connection to that service, the hardware product itself is little more than a simple pedometer. Unless a user can hack the device, which requires some technical sophistication,[70] Fitbit data is not available separate from Fitbit's online services. Likewise, the Philips Directlife device depends even more obviously on a subscription model. The device comes bundled with a one-year subscription for $149, and each additional year of service costs an additional $149.[71] To use the physical device—called the Activity Monitor—users must activate an online account on the DirectLife website. Similarly, BodyMedia's armbands—which operate much like the Fitbit and DirectLife devices—cost $149 to purchase but $6.95 per month for a subscription to BodyMedia's web-enabled data services.[72]

We see this business model elsewhere. Amazon, for example, sells its popular Kindle e-book reader at a loss because of the potential value it sees in electronic media users purchasing from Amazon with the device.[73] It is not clear whether firms like Fitbit, DirectLife, and BodyMedia absorb a loss on the sale of their hardware in order to secure subscriptions. It is obvious, however, that locking users in to long-term service plans is already becoming a dominant strategy in the self-surveillance industry.[74] The Evoz infant monitoring service, for example, is $39.99 per year; Evoz Premium, which includes the ability to receive a message when your infant is crying, costs $69.99 per year.[75]

---

69. *See About Fitbit Premium*, FITBIT, http://www.fitbit.com/premium/about (last visited Aug. 12, 2012).

70. *See, e.g.*, Eric Blue, *Fitbit Hacks: Unofficial API & Tools To Get the Most Out of Your Fitbit*, EIRC BLUE'S BLOG, http://eric-blue.com/projects/fitbit (last visited Aug. 12, 2012) (explaining various Fitbit hacking techniques).

71. *See Shop*, PHILIPS DIRECTLIFE, https://www.directlife.philips.com/shop-us/products/philips-directlife (last visited Aug. 12, 2012).

72. *See Why a Subscription?*, BODYMEDIA, http://www.bodymedia.com/Products/Learn-More/Subscription (last visited Aug. 12, 2012).

73. *See* Diane Mermigas, *Kindle Strategy Fires Amazon's Future*, BUS. INSIDER (Oct. 3, 2011), http://articles.businessinsider.com/2011-10-03/tech/30234692_1_amazon-web-services-ceo-jeff-bezos-largest-online-retailer.

74. Not all manufacturers have adopted the subscription model. Nike, for example, sells the Nike+ Fuelband, which is a bracelet that operates much like Fitbit and DirectLife. Nike makes online data analysis available to Fuelband users without charge. *See Nike+ Fuelband*, NIKE, http://store.nike.com/us/en_us/?l=shop,fuelband (last visited Aug. 12, 2012). This may be a somewhat unique case, however, because Nike is clearly promoting a family of electronic monitoring devices—including GPS watches, enhanced iPods, etc.—in an effort to tie users to Nike's athletic wear and sneakers. In other words, Nike's economics are likely to be quite different than a stand-alone firm like Fitbit.

75. *See Choose Your Evoz Plan*, EVOZ, http://myevoz.com/subscriptions (last visited Aug. 12, 2012).

If a firm adopts this business model, will it be willing to work with a Personal Data Guardian that controls a user's data? Most likely not. Doing so would complicate the firm's strategy of providing data services to the user over time. Although it might be possible for a firm to sell a consumer hardware device *and* sell data analysis for that device without actually seeing the data in question (because the data were locked in a data vault controlled by a Personal Data Guardian), I predict that firms will resist this. Losing access to their users' data would make product testing and quality control more difficult, as well as liberate the consumer to go elsewhere for the long-term data services on which these firms seem to be betting their future. Finally, how is a consumer holding a blood pressure monitor or other tracking device at a Wal-Mart or an Apple store supposed to introduce a Personal Data Guardian to the manufacturer of that device? There does not seem to be much room for negotiation.[76]

Not surprisingly, these device manufacturers have begun to use their terms of service and privacy policies to take ownership and control of the biometric data produced through self-surveillance. Consider just one example: the BodyMedia armband and associated "Activity Manager," which is BodyMedia's web-based data storage and analysis service. BodyMedia's privacy policy states that "[a]ll data collected including, but not limited to, food logs, weight, body-fat percentage, sensor data, time recordings, and physiological data . . . are and shall remain the sole and exclusive property of BodyMedia."[77] The policy goes on to clarify that "[y]ou opt-in to armband-data recording by voluntarily wearing the armband," and that "[y]ou opt-in to self reporting data by voluntarily self reporting information."[78] In other words, if you use your BodyMedia armband, you have contractually relinquished any claim to ownership of, or control over, the data it produces. Other biometric device manufacturers take the same approach.[79]

SSP's authors, of course, may argue that this kind of example proves exactly why Personal Data Guardians are necessary. I agree that such contracts demonstrate the need for solutions, but suggest that they also at

76. Granted, if enough consumers sought to use the Personal Data Guardian model, perhaps market pressure would build for devices equipped to accommodate this architecture. Given the current growth in and popularity of self-surveillance devices *without* such protections, however, and the generally limited apparent demand among consumers for increased privacy protections in other areas, this seems somewhat unlikely.

77. *Privacy Policy*, BODYMEDIA, http://www.bodymedia.com/support-help/policies/privacy-policy (last visited Aug. 12, 2012).

78. *Id.*

79. For example, the Basis sports watch monitors heart rate and other biometric information. The Basis privacy policy makes clear that "[a]ll Biometric Data shall remain the sole and exclusive property of BASIS Science, Inc.," and that "[w]e may share or sell aggregated, de-identified Biometric Data." *Basis Privacy Policy*, BASIS, http://en.mybasis.com/legal/privacy (last visited Aug. 12, 2012).

least partly undermine *SSP*'s premise that self-surveillance involves few or no contractual or third-party complications. The reality on the ground—at least in the Generation Two consumer context—is that self-surveillance is not going to be so pure. Instead, I think we must face the question that *SSP* deems "harder"[80] and thus tries to avoid: how to regulate or manage the creation of such data when there *are* competing legal claims to its ownership and use, especially when the contracts governing such claims are rarely read or understood by consumers?[81]

B. How To Prevent the Unraveling of Privacy?

In addition to these complications about introducing a Personal Data Guardian, I must also question the efficacy of the Personal Data Vault. Assume for a moment that an individual is able to use a guardian to sequester her self-surveillance data in a secure vault. *SSP* seems to assume that once such data are so secured, an individual will be free to then do what she wishes with those data—free to keep such information concealed, on the one hand, or to consent to its revelation, on the other.

I have recently argued at length that such consent may become illusory in certain contexts because of the unraveling effect.[82] Unraveling works as follows. Imagine a pool of people, each of whom knows his or her blood pressure but none of whom knows anyone else's blood pressure. A health insurer offers a discount on insurance premiums if one wears a tiny patch on one's skin that monitors one's blood pressure and wirelessly uploads that information to the insurer daily. There is no obligation to participate—the program is marketed as a way to save by getting a discount if your blood pressure is particularly healthy. (One can generalize this example to any other kind of sensor-observable health trait, such as pulse, exercise history, miles walked or ran, etc.)

What will happen? The unraveling effect teaches that as individuals with very good blood pressure sign up for the monitoring program in order to get a discount, over time others with less good vital signs will increasingly feel pressure to follow suit. If you have middling blood pressure and all those with better health have already signed up, you will be pooled by the insurance companies with those other non-disclosing insureds who have

---

80. Kang et al., *supra* note 1, at 843–44.

81. One might argue that if a Personal Data Guardian is introduced, these firms will find other business models to continue to produce their products. For example, Fitbit might sell its health monitor at a lower cost if a user signs up for Fitbit's data services, but at a much higher price point if a user wants to route the data through a Personal Data Guardian and not use Fitbit's services. The market could give users choices, at different prices, of their preferred privacy approach. This is a possible outcome, but I have my doubts that these firms will be so flexible. The question is whether these firms see themselves as consumer electronics companies or as data management and services companies, and whether they will insist on closely tying their hardware to their data services.

82. *See* Peppet, *supra* note 2, at 1176–90.

poorer health than you. You will therefore disclose, even if your physical condition is not the very best. And so on down the line, as individuals of all types realize that the stigma of *not* disclosing their characteristics has become worse than the penalties that may attach to self-revelation of even poor-to-middling qualities.[83]

Without re-hashing this entire argument here, it suffices to say that locking one's information in a data vault does not relieve the economic pressure one may feel to reveal it to one's economic counterparts. Indeed, in the consumer self-surveillance context, the tie-in to insurance has already begun. Products like Fitbit, DirectLife, BodyMedia, Striiv, and others produce data that is inherently valuable to health insurers, who are always seeking new ways to more precisely track and evaluate the risk characteristics of their insureds. Self-surveillance data is not just useful for self-awareness or self-knowledge; it is also an extremely valuable commodity.

Some consumer self-surveillance firms are thus focusing on the corporate or insurance tie-in as a primary source of revenue. Limeade, for example, offers health monitoring services. Their business model is to sell their services to employers as part of corporate wellness programs. This tie-in to corporate wellness programs is explicit. Limeade's privacy policy provides for sharing a user's information with "third parties who are contracted with your employer or your health plan in order to provide disease management, health management, behavioral coaching, or similar wellness-related services."[84] In addition, Limeade's policy states that an employer or health plan may provide a user "with incentives and rewards for [a user's] participation in the service."[85]

Philips DirectLife is likewise governed by a privacy policy providing that "[w]here you are using DirectLife Products and/or Services as a result of your employment or where your employer is our business partner, we may share with your employer some of your Personal Data."[86] The policy then clarifies that DirectLife will not share "activity level" data (e.g., how much exercise you engaged in, etc.) without a user's consent, except "on an

83. For a much more in-depth discussion of the unraveling effect, see Peppet, *supra* note 2, at 1176–90.

84. *Privacy Policy*, LIMEADE, https://limeade.com/Privacy.aspx (last visited Aug. 12, 2012) [hereinafter *Limeade Privacy Policy*]. For another example of a similar service, see THECARROT.COM, http://www.thecarrot.com (last visited Aug. 12, 2012). The Carrot's terms and conditions of use make it clear that the company can share a user's information with business partners, including employers and insurance companies. *See Terms of Use*, THECARROT.COM, http://thecarrot.com/company/terms (last visited Aug. 12, 2012).

85. *Privacy Policy*, LIMEADE, *supra* note 84.

86. *DirectLife Privacy Notice*, PHILIPS DIRECTLIFE, http://www.directlife.philips.com/privacy_notice (last visited Aug. 12, 2012).

anonymized and aggregated basis."[87] The policy provides for similar sharing with a user's insurance company.[88]

These firms are attempting to build business by offering such data to employers and insurance companies as wellness services. In practice, this means that employers and insurers can now offer discounts and incentives to their employees and/or insureds for revealing self-surveillance data. Locking these data away in a data vault may thus become extremely expensive—not (only) because of the cost associated with paying a Personal Data Guardian to maintain a Personal Data Vault, but because of the inherent penalties one may begin to pay in health insurance premiums for refusing to reveal such data. In short, it may not be worth it to try to secure such information as we increasingly inhabit a world in which the economy demands its subsequent revelation.

C. *What About Regulating Consumer Device Makers as Privacy Intermediaries, Rather than Trying To Create New Privacy Agents?*

It pains me to argue that Personal Data Guardians may not work in practice. I want them to succeed. Structural solutions like this seem to me the best way to re-engineer the flow of personal information to secure greater privacy. At the same time, if the two objections raised to this point hold weight, then *SSP*'s core prescriptions do not. We may not be able to lock away sensor-based self-surveillance data, even if we were to create a profession of Personal Data Guardians and a system of secure Personal Data Vaults.

What then to do about such data? As indicated at the start, *SSP* is clearly correct to draw attention to the increase in both quantity and quality of such information.[89] We can now measure all sorts of biometric markers, and the quantification of the self will only increase in sophistication.[90] But it seems that—for good or ill—the consumer devices and applications that will bring such self-measurement to the general population will be enmeshed in a legal and economic context far messier than that described or proposed by *SSP*. Instead, we will have to continue to wrestle with the fact that much self-surveillance data will be collected, stored, analyzed, and used not by privacy *agents*, but by firms serving as *intermediaries* between the individuals using self-surveillance sensor technologies and other economic actors—such as advertisers, health insurers, and employers—that want and will pay for at least some access to such data.

---

87. *Id.*

88. *See id.*

89. *See supra* notes 7–42 and accompanying text.

90. For a stunning example of where we are headed, see the explanatory video at scanadu.com. SCANADU, http://www.scanadu.com/ (last visited Aug. 12, 2012) (describing Scanadu's experimental Tricorder health-monitoring system).

Firms that collect consumers' self-surveillance data are thus akin to Google, Facebook, and a host of other existing internet intermediaries about which privacy scholars have begun to express doubts.[91] Unlike agents, such as *SSP*'s Personal Data Guardians, that can have clear and unconflicted fiduciary obligations to an individual, intermediaries present a muddier situation. They may be obligated to their individual users, but they may be paid by the advertisers, insurers, or others on the "other side" of the economic transactions. They may say they wish to protect a user's privacy, but have every incentive not to do so. And unlike *SSP*'s proposed privacy agents, they may not be particularly transparent about their incentives, intentions, or conflicts.

Nevertheless, if the agency-based model proposed by *SSP* does not gain traction—and, as explained, I have reason to doubt that it can—we may be stuck with acknowledging that consumer-scale Generation Two self-surveillance will be managed by firms serving as intermediaries instead. To the extent one believes that greater privacy protections are needed, we may therefore have to define the obligations of such "privacy intermediaries" in greater detail, and begin to regulate this class of intermediaries more heavily—as we have regulated intermediaries in the financial and other contexts. How best to do so is a topic for another day.

91. *See, e.g.*, Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 NW. U. L. REV. 105 (2010).