2011

Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future

Scott R. Peppet
University of Colorado Law School

Printed in U.S.A.
Vol. 105, No. 3

UNRAVELING PRIVACY: THE PERSONAL PROSPECTUS AND THE THREAT OF A FULL-DISCLOSURE FUTURE

Scott R. Peppet[*]

As for privacy in general, it is difficult to see how a pooling equilibrium is avoided in which privacy is 'voluntarily' surrendered, making the legal protection of privacy futile.[†]

INTRODUCTION

Every day that Tom Goodwin drives his Chevy Tahoe, his insurance company uses a small electronic monitor in his car to track his total driving time, speed, and driving habits. If he drives less than ten thousand hours a year, does not drive much after midnight, and avoids frequently slamming on the brakes, at the end of the year he receives up to twenty-five percent

---

[*] Associate Professor of Law, University of Colorado School of Law. I thank Ryan Calo, Danielle Citron, Vic Fleischer, Paul Ohm, and Phil Weiser for their feedback on this project, as well as the participants in the University of Colorado School of Law's faculty workshop. I thank Mark Gibson and Matt Burns for their excellent research assistance.

[†] Richard Posner, *Privacy*, *in* 3 THE NEW PALGRAVE DICTIONARY OF ECONOMICS & THE LAW 103, 107 (Peter Newman ed., 1998).

off his premiums. "There's this 'Big Brother' thing, but it's good," Goodwin says. "Since I know I'm being watched, I'm on my best behavior."[1] To date, Progressive Insurance's MyRate program is available in forty states and has enrolled roughly ten thousand customers.[2] Other insurance companies are following suit.[3] Some carriers go even further, offering discounts for the use of more sophisticated devices that record geographical location, minute-by-minute speeding violations, and seat belt usage.[4] Rental car companies have also experimented with using such monitors to incentivize safe driving.

Similarly, the Mayo Clinic in Rochester, Minnesota, uses remote monitoring devices every day to check up on the health of residents at Charter House, a nearby senior living center. The devices transmit data about irregular heart rhythms, breathing rates, and the patients' positions and motions. "The goal," says Dr. Charles Bruce, an investigator on the project, "is to have full remote monitoring of people . . . just like you measure the pressure of your tires today."[5] Medical device companies are racing to enter the remote monitoring space. Proteus Biomedical, for example, is testing a wearable electronic device that can sense when patients have taken their pills and transmit that information to the patients' doctors.[6] GlySens is working on an implantable subcutaneous blood sugar sensor for diabetics that uses wireless communication that could be used to constantly send real-time results to their doctors.[7] FitBit, BodyMedia, Toumaz, and other com-

---

[1] Bengt Halvorson, *Car Insurance Savings Come with 'Big Brother,'* CNN (May 22, 2009, 9:28 AM), http://www.cnn.com/2009/LIVING/wayoflife/05/22/aa.pay.as.drive.insurance.

[2] The program was recently renamed Snapshot and updated slightly. *See Snapshot Discount*, PROGRESSIVE.COM, http://www.progressive.com/myrate (last visited Jan. 30, 2012).

[3] Many insurance providers offer similar discounts, sometimes of up to sixty percent off regular premiums. *See* Jilian Mincer, *To Your Benefit*, WALL ST. J., Dec. 7, 2009, at R10 (discussing various plans). GMAC Insurance, for example, uses OnStar data to track total miles driven. *See The GMAC Insurance Low-Mileage Discount*, GMAC INS., http://www.gmac123.com/auto-insurance/smart-discounts/low-mileage-discount.asp (last visited Jan. 30, 2012).

[4] *See Parents Help Keep Teen Drivers Safe with DriveSmart*, ANPAC, http://www.anpac.com/DriveSmart/WhatIsDriveSmart/FAQ/default.aspx (last visited Jan. 30, 2012). Intel is working on more sophisticated monitoring systems for cars akin to the "black boxes" in aircraft, capable of recording and transmitting basic vehicle telemetry, seat belt usage, geographical location, mechanical malfunctions, and video of auto accidents, all of which would be of great interest to an insurance carrier. *See* John R. Quain, *Intel Working on Black Box for Your Car*, N.Y. TIMES (July 7, 2010, 11:05 AM), http://wheels.blogs.nytimes.com/2010/07/07/intel-working-on-black-box-for-your-car. Last year, Congress introduced legislation to make such event recorders mandatory in all new cars. *See* Motor Vehicle Safety Act of 2010, S. 3302, 111th Cong. § 107. For discussion of the privacy implications of such technologies, see Patrick R. Mueller, Comment, *Every Time You Brake, Every Turn You Make—I'll Be Watching You: Protecting Driver Privacy in Event Data Recorder Information*, 2006 WIS. L. REV. 135.

[5] Steven Rogerson, *The Mayo Clinic Trials Health's New Big Brother*, MEDICALDEVICE-NETWORK.COM (Apr. 15, 2010), http://www.medicaldevice-network.com/features/feature81227.

[6] *See* Don Clark, *Take Two Digital Pills and Call Me in the Morning*, WALL ST. J., Aug. 4, 2009, at A6.

[7] *See* Keith Darcé, *S.D. Company Hopes Monitor Will Revolutionize Diabetes Care*, SIGN ON SAN DIEGO (July 28, 2010, 9:13 PM), http://www.signonsandiego.com/news/2010/jul/28/sd-company-hopes-

panies market devices that track physical activity, calories burned, sleep habits, and other data.[8] Although today these devices do not report data to users' health insurers, it would be a simple step for a patient to provide such access in return for a discount. Indeed, the health care community is already discussing such "pervasive lifestyle incentive management."[9]

Finally, tenants, job applicants, and students voluntarily disclose verified personal information to their prospective landlords, employers, and universities every day using online services such as MyBackgroundCheck.com.[10] Rather than forcing these entities to run a background check, an applicant can digitally divulge pre-verified information such as criminal record, sex offender status, eviction history, and previous rental addresses. Moreover, these services allow an applicant to augment her resume by having verified drug testing done at a local collection site and added to her digital record. MyBackgroundCheck.com calls this feature "resume enhancement."[11]

This Article makes three claims. *First*, these examples—Tom Goodwin's car insurance, pervasive health monitoring, and the incorporation of verified drug testing into one's "enhanced resume"—illustrate that rapidly changing information technologies are making it possible for consumers to share verified personal information at low cost for economic reward or, put differently, for firms to extract previously unavailable personal information from individuals by offering economic incentives. In this world, economic actors do not always need to "sort" or screen each other based on publicly available information; instead, they can incentivize each other to "signal" their characteristics. For example, an insurance company does not need to do extensive data mining to determine whether a person is a risky driver or an unusual health risk—it can extract that information from the insured directly. *Second*, this change towards a "signaling economy," as opposed to the "sorting economy" in which we have lived since the late 1800s, poses a very different threat to privacy than the threats of data mining, aggregation,

---

monitor-will-revolutionize. There are already regular finger-prick blood sugar monitors that transmit such data electronically after each reading. *See Products—IDEAL LIFE Gluco Manager™*, IDEAL LIFE, http://www.ideallifeonline.com/products/glucomanager (last visited Jan. 30, 2012).

[8] *See* FITBIT, http://www.fitbit.com (last visited Sept. 4, 2011) (selling Fitbit Tracker); *Home—SenseWear*, BODYMEDIA, INC., http://sensewear.bodymedia.com (last visited Jan. 30, 2012) (marketing the BodyMedia SenseWear system); *Toumaz—Sensium Introduction*, TOUMAZ, http://www.toumaz.com/page.php?page=sensium_intro (last visited Jan. 30, 2012) (describing the Toumaz Sensium platform for real-time body monitoring).

[9] *See, e.g.*, Upkar Varshney, *Pervasive Healthcare and Wireless Health Monitoring*, 12 MOBILE NETWORKS & APPLICATIONS 113, 115 (2007) ("Pervasive lifestyle incentive management could involve giving a small mobile micro-payment to a user device every time the user exercises or eats healthy food." (emphasis omitted)).

[10] *See* MYBACKGROUNDCHECK.COM, http://www.mybackgroundcheck.com (last visited Jan. 30, 2012).

[11] *See Schedule a Drug Test for Yourself and Share the Results*, MYBACKGROUNDCHECK.COM, http://www.mybackgroundcheck.com/DrugTesting.aspx (last visited Sept. 4, 2011).

and sorting that have preoccupied the burgeoning field of informational privacy for the last decade. In a world of verifiable information and low-cost signaling, the game-theoretic "unraveling effect" kicks in, leading self-interested actors to fully disclose their personal information for economic gain. Although at first consumers may receive a discount for using a driving or health monitor, privacy may unravel as those who refuse to disclose are assumed to be withholding negative information and therefore stigmatized and penalized. *Third*, privacy law and scholarship must reorient towards this unraveling threat to privacy. Privacy scholarship is unprepared for the possibility that when a few people have the ability and incentive to disclose, everyone may ultimately be forced to do so. The field has had the luxury of ignoring unraveling because technologies did not exist to make a signaling economy possible. Those days are over. As the signaling economy emerges, privacy advocates must either concede defeat or focus on preventing unraveling. The latter requires both a theoretical shift in our conception of privacy harms and practical changes in privacy reform strategies.

This Article addresses these claims in its three parts. Part I explores the emerging signaling economy. In the signaling economy, individuals and firms can extract verified, high-quality, low-cost data from each other directly rather than searching through mountains of unverified, low-quality information. Developments in information technology make information increasingly verifiable, and thus increasingly valuable as signals, especially in situations in which there is information asymmetry. I propose a simple metaphor to capture the extreme possibilities of this signaling economy: the "personal prospectus." The personal prospectus would be a compilation of an individual's verified private information about himself: a digital repository containing the data collected from the sensors and drug tests in the previous examples, or from the many other innovative monitors undoubtedly around the corner, as well as information from one's bank accounts, educational records, tax history, criminal history, immigration records, health records, and other private sources. It might include one's eBay Feedback score or Klout score.[12] In short, it would be the aggregate of all of one's private tests, records, and history in a single massive digital resume, shareable with others at the click of a button. The personal prospectus provides a useful means to explore the limits and possibilities of this new signaling economy, and it also illustrates the shortcomings of existing privacy law and scholarship.

Part II takes up the Article's second claim: that even the first steps that we are now taking towards a signaling economy pose a new set of privacy

[12] EBay Feedback scores measure the satisfaction of one's prior transaction partners. *See How Feedback Works*, EBAY, http://pages.ebay.com/help/Feedback/howitworks.html (last visited Jan. 30, 2012). A Klout score is a measure of one's influence on various social media platforms such as Facebook and Twitter. *See* KLOUT, http://www.klout.com (last visited Jan. 30, 2012).

challenges previously largely ignored. Judge Richard Posner first articulated these challenges decades ago although at the time they seemed more theoretical than practical.[13] Even with control over her personal information, he argued, an individual will often find it in her self-interest to disclose such information to others for economic gain. If she can credibly signal to a health insurer that she does not smoke, she will pay lower premiums. If she can convince her employer that she is diligent, she will receive greater pay. As those with positive information about themselves choose to disclose, an "unraveling effect" will occur: in equilibrium, *everyone* will disclose their information, whether positive or negative, because disclosure by those with the best private information leads to disclosure even by those with the worst.

The classic example of unraveling imagines a buyer inspecting a crate of oranges.[14] The quantity of oranges in the crate is unknown, and opening the crate before purchase is unwise because the oranges will rot before transport. There are stiff penalties for lying, but no duty on the part of the seller to disclose the number of oranges in the crate. The number of oranges will be easy to verify once the crate is delivered and opened. The buyer believes that there cannot be more than one hundred oranges.

The economic theory of unraveling posits that each seller will fully disclose the number of oranges in her crate, regardless of how many it contains. Begin with the choice faced by a seller with one hundred oranges in her crate. If the seller stays silent, the buyer will assume that there are fewer than one hundred oranges and will be unwilling to pay for the full amount. The seller with one hundred oranges will therefore disclose and charge full price. Now consider the choice of a seller with ninety-nine oranges. If this seller stays quiet, the buyer will assume that there are fewer than ninety-nine oranges and will discount accordingly. Because a silent seller is pooled with every lower-value seller, staying silent works to his disadvantage. He will therefore disclose.

And so it goes, until one reaches the seller with only one orange and the unraveling is complete. As Douglas Baird, Robert Gertner, and Randal Picker put it, "Silence cannot be sustained because high-value sellers will distinguish themselves from low-value sellers through voluntary disclosure."[15] In his classic text, *Passions Within Reason*, economist Robert Frank coined the term the "full disclosure principle" to describe this phenomenon. The principle is simple: "if some individuals stand to benefit by

---

[13] Judge Posner's clearest description of this problem is in Posner, *supra* note †, at 105–07. He began to develop these themes in RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 234 (1981).

[14] This example is drawn from S.J. Grossman & O.D. Hart, *Disclosure Laws and Takeover Bids*, 35 J. FIN. 323, 324 (1980). It has been repeated since. *E.g.*, DOUGLAS G. BAIRD, ROBERT H. GERTNER & RANDAL C. PICKER, GAME THEORY AND THE LAW 89–90 (1994) (using this example); Robert H. Gertner, *Disclosure and Unravelling*, *in* 1 THE NEW PALGRAVE DICTIONARY OF ECONOMICS & THE LAW, *supra* note †, at 605, 605 (same).

[15] BAIRD, GERTNER & PICKER, *supra* note 14, at 90.

revealing a favorable value of some trait, others will be forced to disclose their less favorable values."[16]

In the years since Posner's challenge, however, privacy law has almost entirely overlooked the threat of unraveling. Instead, recent informational privacy scholarship[17] has focused on the privacy threats from firms sorting individuals by mining aggregated data such as credit histories. Informational privacy law has reacted to sorting becoming more commonplace and sophisticated.[18] The field is dominated by Daniel Solove's concept of the "digital dossier," which is a metaphor for the aggregate of information available in public and private databases about a given person.[19] Privacy scholars fear that we are moving towards a world in which everything becomes public and all of our personal information becomes easily available to others as part of our digital dossier.[20] Accordingly, the literature is filled with calls to give individuals greater control[21] over their personal information through the common law of property and tort and through stronger statutory privacy rights.[22]

The personal prospectus poses a different threat than Solove's digital dossier, however, and it demands different solutions than increased control over one's information. *In a signaling economy, even if individuals have control over their personal information, that control is itself the undoing of their privacy.* Because individuals hold the keys, they can be asked—or forced—to unlock the door to their personal information. Those who refuse to share their private information will face new forms of economic discrim-

---

[16] ROBERT H. FRANK, PASSIONS WITHIN REASON 104 (1988).

[17] *See* Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087 (2006) (reviewing DANIEL J. SOLOVE, THE DIGITAL PERSON (2004)) (discussing the field of informational privacy law).

[18] *See infra* Part II.B.

[19] *See* SOLOVE, *supra* note 17, at 1–2 (defining the digital dossier).

[20] *See* Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 55–56 (2007) (demonstrating the ease of obtaining a digital dossier on a person); John Palfrey, *The Public and the Private at the United States Border with Cyberspace*, 78 MISS. L.J. 241, 244 (2008) (discussing growth of the digital dossier); Lee Tien, *Privacy, Technology and Data Mining*, 30 OHIO N.U. L. REV. 389, 398–99 (2004) (explaining the risks that digital dossiers pose to privacy and associational freedom).

[21] Control has been the dominant American definition of privacy. *See, e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967); Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) ("Privacy . . . is the *control* we have over information about ourselves."); Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890) ("The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."). Control is also the dominant prescribed remedy for privacy violation. *See, e.g.*, Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 820 (2000) ("The weight of the consensus about the centrality of privacy-control is staggering."); Sonja R. West, *The Story of Us: Resolving the Face-Off Between Autobiographical Speech and Information Privacy*, 67 WASH. & LEE L. REV. 589, 606 (2010) ("[I]t is the control over the disclosure of information . . . that lies at the heart of the legal protection for information privacy.").

[22] *See infra* Part II.B.

ination. How long before one's unwillingness to put a monitor in one's car amounts to an admission of bad driving habits, and one's unwillingness to wear a medical monitor leads to insurance penalties for assumed risky behavior? In a signaling economy, forced disclosure will be at least as difficult a problem as data mining and the digital dossier.

Consider another example: the unraveling strategy of Global Rainmakers, Inc. (GRI), a biometrics company currently engaged in a massive test rollout of iris scanners across the city of Leon, Mexico.[23] These scanners cost roughly $50 to $100 per device. GRI is working with the city of Leon to deploy thousands of scanners over several years to control access to medical centers, banks, public transportation, automatic teller machines, and many other aspects of daily life. In the first stage of deployment, all convicted criminals will be required to submit for iris scanning. But GRI expects that others will quickly volunteer to take advantage of the conveniences that the system affords.[24] Ultimately, however, unraveling may lead to full participation and full disclosure, even by those that might at first hesitate for fear that their checkered personal histories will be used to discriminate against them by, e.g., barring access to a mall or high-end shop. As Jeff Carter, Chief Development Officer of GRI, put it, "When you get masses of people opting-in, opting out does not help. Opting out actually puts more of a flag on you than just being part of the system. We believe everyone will opt-in."[25] In other words, in a signaling economy, the stigma of nondisclosure may be worse than the potential discriminatory consequences of full disclosure.

Part III thus attempts to reorient informational privacy law towards the growing threats of signaling and unraveling. Unlike Judge Posner, however, I do not assume that unraveling necessarily leads to the end of privacy. Instead, Part III explores both the economic conditions necessary for unraveling and the legal means available to constrain it. In particular, Part III examines the three possible legal responses to the unraveling of privacy—"don't ask," "don't tell," and "don't use" rules—and explores their limitations and implications. I conclude that, although it is possible to constrain the unraveling of privacy, it will require privacy advocates to move well beyond their traditional focus on increasing individual control over information. Instead, the privacy field must wrestle directly with the problems of paternalism inherent in limiting the use of information that at least some consumers may *want* to disclose for economic advantage.[26] Limiting blood

---

[23] *See* Austin Carr, *Iris Scanners Create the Most Secure City in the World. Welcome, Big Brother*, FAST COMPANY (Aug. 18, 2010), http://www.fastcompany.com/1683302/iris-scanners-create-the-most-secure-city-in-the-world-welcomes-big-brother.

[24] *Id.*

[25] *Id.*

[26] For an excellent discussion, see Anita L. Allen, *Unpopular Privacy: The Case for Government Mandates*, 32 OKLA. CITY U. L. REV. 87, 89–90 (2007), which discusses ways in which government requires unpopular privacy, such as regulating that erotic dancers wear pasties or G-strings despite their

glucose monitoring by insurers may protect the privacy of the least healthy diabetics who might otherwise be forced to disclose by the unraveling effect, but such limits would also impose costs on the most healthy and conscientious patients who would otherwise receive discounts for wearing a glucose monitor. How will legislatures respond to consumer pressure *for* the right to disclose? If to date the informational privacy field has been unable to muster legislative support even for increasing control over personal data, how persuasive will it be when faced with these more difficult prescriptive debates?

Part III offers the first comprehensive exploration of these questions. This discussion is timely, because as the signaling economy develops, courts and legislatures are increasingly wrestling with these problems.[27] The most prominent example is the recent health care bill, the Patient Protection and Affordable Care Act (PPACA).[28] Incentive-based health insurance premiums were a central battleground in the give-and-take leading up to the PPACA's passage. The PPACA's section 2705 increases the degree to which employers and insurers can use discounts on health insurance premiums to incentivize employees to participate in wellness programs and to try to achieve specified personal health goals.[29] Disease advocacy groups fought for various limitations on the use of incentives,[30] but privacy advocates were largely absent from the debate. The privacy field seems to have assumed that the only privacy issues in the bill arose in the context of the use and security of electronic health records.[31] This is a mistake. Incentives to signal raise exactly the questions to which informational privacy law must turn: questions of justice, fairness, paternalism, and power; questions about coercion and the limits of "voluntary" disclosure; questions, in short, about how to deal with the threat of unraveling privacy.

---

belief that they could maximize profits through full disclosure. *See also* ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? (2011).

[27] Examples include litigation and legislation over the use of radio frequency identification tags, location-monitoring devices in rental cars, and health care incentives. *See infra* Part I.C.

[28] Patient Protection and Affordable Care Act of 2010, Pub. L. No. 111-148, 124 Stat. 119.

[29] *Id.* § 2705; *see infra* note 80–84 and accompanying text.

[30] *See* Michael P. O'Donnell, *Editor's Notes*, 24 AM. J. HEALTH PROMOTION, at iv, iv (2010).

[31] Privacy advocates' main focus has been on the privacy and security of electronic health records. Comparatively little attention has been paid to the privacy issues implicit in incentive programs. *See, e.g.*, PATIENT PRIVACY RIGHTS, http://patientprivacyrights.org (last visited Jan. 30, 2012) (illustrating little discussion of incentive provisions by privacy advocates).

I. THE PERSONAL PROSPECTUS AND THE EVOLUTION OF A SIGNALING ECONOMY

A. Sorting and Signaling

It is often difficult to distinguish the trustworthy from the untrustworthy, the good from the bad, the high quality from the low. If you are choosing a business partner, you might value honesty and diligence, but you also face the difficulty of determining whether your potential partner actually has these traits or is just putting on a good show to lure you into the deal. If you are purchasing a car, how do you determine whether it is dependable or a lemon?[32]

These asymmetric information problems—how to distinguish one desirable "type" of people, goods, or assets from another less desirable type—have occupied economists and legal scholars for decades. Consider the simple decision of whether to lend money to Alice or Bob. If you could easily determine that Alice is more creditworthy, you would choose to do business with Alice and not Bob or, at least, to charge Bob a greater interest rate than Alice. If you cannot so distinguish, however, you will either lend to neither or charge both the higher interest rate because you must cover for the possibility that both are of the undesirable type that is likely to default.[33] This creates extra costs for Alice and Bob, inefficiencies for you, and a burden on the economy generally.[34] If the market cannot absorb these costs, creditworthy Alices may be priced out of the market completely.[35]

Sorting and signaling are the two primary economic devices to overcome such information asymmetries.[36] Sorting, or "screening," theory assumes that, if the desired characteristic is unobservable, an uninformed party will filter counterparties based on what observable characteristics or information *is* available.[37] For example, a lender might use job turnover, prior bankruptcies, or a poor credit score as proxies for future default risk.

---

[32] *See* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488, 489 (1970).

[33] *See generally* Dwight M. Jaffee & Thomas Russell, *Imperfect Information, Uncertainty, and Credit Rationing*, 90 Q.J. ECON. 651, 651–52 (1976) (describing the dynamics of credit markets under low-information conditions).

[34] *See* Joseph E. Stiglitz & Andrew Weiss, *Credit Rationing in Markets with Imperfect Information*, 71 AM. ECON. REV. 393, 393–94 (1981).

[35] *See* Akerlof, *supra* note 32, at 490–91.

[36] For an overview of sorting and signaling, see John G. Riley, *Silver Signals: Twenty-Five Years of Screening and Signaling*, 39 J. ECON. LITERATURE 432 (2001).

[37] *See, e.g.*, Roger Klein, Richard Spady & Andrew Weiss, *Factors Affecting the Output and Quit Propensities of Production Workers*, 58 REV. ECON. STUD. 929 (1991) (exploring the example of employers sorting job applicants based on high school graduation as a proxy for perseverance).

Signaling is the counterpart to sorting.[38] Economic actors use signals to qualitatively distinguish themselves from other economic actors. Signaling "refers to actions taken by an informed party for the sole purpose of credibly revealing his private information."[39] In our credit example, if there are two types of borrowers seeking funds, Alice and Bob, and Alice is likely to pay back whereas Bob is not, Alice has incentive to reveal her trustworthiness to the lender to receive a lower interest rate.

Alice may try to signal her type by simply saying, "I am a good credit risk—I will repay my loans," but talk is cheap.[40] The lender will doubt Alice because Alice has every reason to lie. Moreover, because it is easy to say such words, both Alice and Bob will say them, and the lender will be no better off than it was before in trying to distinguish Alice from Bob. These are the situations that incentivize lenders to mine for data and base lending decisions on the basis of personal information that they can uncover about borrowers.

To ensure that she gets the lower rate that she deserves in a signaling economy, however, Alice may disclose information that can be used as a proxy of future creditworthiness, such as her income level or employment history. For such disclosure to be an effective signal, the disclosed information must be verifiable. Such verification has been costly in an economy based on offline information.[41] An economic actor seeking to rely on a piece of information must expend time and resources to verify it by, for example, calling references, checking employment or tax records, or calling to verify educational achievements. Although such steps are effective in some

---

[38] *See* Michael Spence, *Informational Aspects of Market Structure: An Introduction*, 90 Q.J. ECON. 591, 592 (1976) ("[Signaling and sorting] are opposite sides of the same coin.").

[39] N. GREGORY MANKIW, PRINCIPLES OF ECONOMICS 487 (5th ed. 2009). Put differently, "adverse selection may give rise to signaling, which is the attempt by the informed side of the market to communicate information that the other side would find valuable." WILLIAM A. MCEACHERN, ECONOMICS 313 (5th ed. 2000).

[40] *See* Joseph Farrell & Matthew Rabin, *Cheap Talk*, J. ECON. PERSP., Summer 1996, at 103, 103–05 (discussing cheap talk generally).

[41] As a result, economists generally focus on signaling devices that are self-verifying by being costly to fake—whereby an action taken by Alice serves in and of itself as a signal of Alice's type. *See* MANKIW, *supra* note 39, at 487 (defining signaling). There are many examples. *See, e.g.*, DIANE COYLE, THE SOULFUL SCIENCE: WHAT ECONOMISTS REALLY DO AND WHY IT MATTERS 163 (rev. ed. 2010) (describing how Indian villagers borrow huge sums to pay for expensive weddings to signal their caste and social status); Paul Herbig & John Milewicz, *Market Signaling Behavior in the Service Industry*, 1 ACAD. MARKETING STUD. J. 35, 39 (1997) (describing how banks and law firms spend vast sums on elaborate office buildings to signal their quality and solvency to potential clients); Robert Puelz & Arthur Snow, *Evidence on Adverse Selection: Equilibrium Signaling and Cross-Subsidization in the Insurance Market*, 102 J. POL. ECON. 236, 237 (1994) (describing how an insured chooses a high-deductible automobile insurance plan, thereby signaling their quality and low risk to the insurance company). Michael Spence began modern signaling theory in Michael Spence, *Job Market Signaling*, 87 Q.J. ECON. 355 (1973). *See also* Michael Spence, *Competition in Salaries, Credentials, and Signaling Prerequisites for Jobs*, 90 Q.J. ECON. 51 (1976) (discussing his classic example of signaling through educational achievement).

instances, they impose costs. When signaling is cost-prohibitive, economic actors will instead rely on sorting.

B. Sorting and the Digital Dossier

The "sorting economy" has developed over the last one hundred fifty years as economic actors have been increasingly able to distinguish desirable counterparties by extracting and sorting information about them. Before turning to the evolving signaling economy in section C, one must first understand the sorting economy and its culmination in today's digital dossier.

The industrial economy had developed sophisticated sorting mechanisms long before the Internet made today's data aggregation and data mining possible. Since the 1800s, the credit industry[42] in particular has aggregated and disseminated information about potential borrowers.[43] Merchants and lenders evolved from knowing each other and their customers personally[44] to relying on merchant associations that exchanged reputational information,[45] to using in-house private investigators to assess trading partners,[46] and ultimately to relying on the credit-reporting agencies that emerged in the mid-1800s.[47] Throughout the 1900s, the number of agencies increased dramatically, and their information-sharing techniques grew more sophisticated and comprehensive.[48]

By the 1970s and 1980s, computer technology made it far easier for credit agencies to collaborate across geographic distances by sharing information, which gave rise to the small number of large credit agencies that

---

[42] *See* Federico Ferretti, *A Historical Primer on Consumer Credit Reporting Systems: A Lesson for EU Policy Makers?*, 12 INT'L J. COMM. L. & POL'Y 92, 95 (2008) (describing how credit information systems "represent an institutional response at the service of the credit industry to the problem of asymmetric information in financial markets").

[43] *See* John M. Barron & Michael Staten, *The Value of Comprehensive Credit Reports: Lessons from the U.S. Experience*, *in* CREDIT REPORTING SYSTEMS AND THE INTERNATIONAL ECONOMY 273 (Margaret J. Miller ed., 2003).

[44] Ferretti, *supra* note 42, at 98 ("The small scale of trade in the US until the early nineteenth century had allowed traders to rely on personal ties or, in the event the seller did not know a prospective buyer personally, on the experiences and opinions of other merchants."); *see also* Josh Lauer, *From Rumor to Written Record: Credit Reporting and the Invention of Financial Identity in Nineteenth-Century America*, 49 TECH. & CULTURE 301, 304, 306 (2008) ("[A]s many discovered, often through disaster, the traditional way of assessing a credit-seeker's trustworthiness—direct experience, word of mouth, and letters of recommendation—proved increasingly unreliable.").

[45] *See* Lauer, *supra* note 44, at 302–03.

[46] *See* Ferretti, *supra* note 42, at 99.

[47] For excellent overviews of nineteenth-century credit-reporting systems, see JAMES D. NORRIS, R.G. DUN & CO., 1841–1900: THE DEVELOPMENT OF CREDIT-REPORTING IN THE NINETEENTH CENTURY (1978); ROWENA OLEGARIO, A CULTURE OF CREDIT: EMBEDDING TRUST AND TRANSPARENCY IN AMERICAN BUSINESS (2006).

[48] *See* Marco Pagano & Tullio Jappelli, *Information Sharing in Credit Markets*, 48 J. FIN. 1693, 1711–12 (1993).

now dominate the American market.[49] In turn, the Internet revolution of the last twenty years allowed information aggregation to explode far beyond the credit markets. It is difficult to overstate the pervasive nature of the data mining and aggregation that feed today's digital dossiers.[50] "Data collection is the dominant activity of commercial websites. Some 92 percent of them collect personal data from web users, which they then aggregate, sort, and use."[51] One scholar has estimated that corporate data mining links at least seven thousand transactions to each individual in the United States per year—approximately half a million transactions over a lifetime.[52] Supermarkets, airlines, hotels, and merchants all track and share information about consumers to better market their products.[53] All of this comprises our digital dossier.

The dominant purpose of this data mining and aggregation is predictive profiling: creating models that can extrapolate from existing data to predict future behavior.[54] In other words, sorting. As Douglas Baird has argued about lenders, for example,

> Advances in data processing allow information about debtors to be collected on a massive scale. It is now possible to look at a particular debtor, identify characteristics such as age, marital status, education, and length of stay at current employer, compare that debtor with others for whom there is a credit history, and make a confident prediction about the likelihood that the debtor will repay a loan.[55]

Beyond credit markets, corporations might explore correlations between past consumer behavior and future purchases, such as whether a person who

---

[49] Prior to the 1970s, the credit bureau industry had largely been fragmented into many local agencies. The onset of the computer revolution eliminated the efficiencies of having a local bureau as opposed to a larger, more regional or national agency, and led to consolidation in the credit agency industry and the emergence of a few large national credit agencies. *See id.* at 1712 ("From a network of local monopolies, credit bureaus began to evolve into a nationwide oligopoly.").

[50] Although the focus here is on data mining by private entities for economic purposes, it is worth noting that governmental data mining and aggregation obviously pose serious risks to privacy. For a discussion of governmental use of such data, see, for example, Ira S. Rubinstein, Ronald D. Lee & Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261 (2008).

[51] LAWRENCE LESSIG, CODE: VERSION 2.0, at 219 (2006).

[52] Jason Millar, *Core Privacy: A Problem for Predictive Data Mining*, *in* LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY 103, 105 (Ian Kerr et al. eds., 2009); *see also* James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1464–65 (2004) (discussing the counterterrorism uses of commercial data and data mining).

[53] *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 596 (2004) (discussing how opportunities for rent-seeking have caused corporations to undertake data-collection efforts).

[54] *See* Millar, *supra* note 52, at 106 (distinguishing descriptive from predictive data mining).

[55] Douglas G. Baird, *Technology, Information, and Bankruptcy*, 2007 U. ILL. L. REV. 305, 312.

had bought both Brand X and Brand Y will also buy Brand Z.[56] An insurance company might use health records to predict life expectancy.[57] An employer might try to extrapolate the likelihood of future success as an employee from the tea leaves of a candidate's past.[58] A merchant might try to predict whether a given customer's check will bounce based on rudimentary information about that check-writer.[59]

The digital dossier is thus the technological culmination of one hundred fifty years of increasingly sophisticated sorting. The upside is that massive data aggregation and computer data analysis create market efficiencies because they allow parties to overcome information asymmetries with greater accuracy and lower cost. The downside is the risk such techniques present to privacy.

Informational privacy scholars have trumpeted the dangers of the sorting made possible by the digital dossier:

> We're heading toward a world where an extensive trail of information fragments about us will be forever preserved on the Internet, displayed instantly in a Google search. We will be forced to live with a detailed record beginning with childhood that will stay with us for life wherever we go, searchable and accessible from anywhere in the world. This data can often be of dubious reliability; it can be false and defamatory; or it can be true but deeply humiliating or discrediting. We may find it increasingly difficult to have a fresh start, a second chance, or a clean slate. . . . This record will affect our ability to define our identities, to obtain jobs, to participate in public life, and more.[60]

---

[56] *See* JOSEPH P. BIGUS, DATA MINING WITH NEURAL NETWORKS 17–18 (1996) (discussing correlation of product purchases); Tal Z. Zarsky, *Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society*, 56 ME. L. REV. 13, 36–37 (2004) (discussing use of data mining to reveal correlations in consumer behavior).

[57] *See* Anita Ramasastry, *Lost in Translation? Data Mining, National Security and the "Adverse Inference" Problem*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 757, 768 (2006) ("Factors such as our credit score are meant to be predictors of how likely we are to repay our loans; likewise, our health, age and other physical characteristics are meant to be predictors of what our life expectancy may be.").

[58] The U.S. market for pre-employment background screening is roughly $2 billion per year. J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 110 (2008). Predicting employee success based on past history is a common use of the digital dossier. *See* Robert Sprague, *Orwell Was an Optimist: The Evolution of Privacy in the United States and Its De-evolution for American Employees*, 42 J. MARSHALL L. REV. 83, 87 (2008) (discussing databases for pre-employment screening).

[59] A merchant can electronically submit a shopper's driver's license or bank information, which can be gleaned from the check itself, and various services compare that information to their databases to provide the merchant with a rating of the check-writer's reliability. *See* Ronald J. Mann, *Information Technology and Non-legal Sanctions in Financing Transactions*, 54 VAND. L. REV. 1627, 1631–32 (2001) (discussing check verification systems).

[60] DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 17 (2007).

This has been the dominant concern of the privacy field for the last decade.[61]

C. *Signaling and the Personal Prospectus*

Despite being the center of attention in privacy law, however, sorting is not the only means available to overcome information asymmetries. The three examples in the Introduction—personal monitoring discounts for car insurance, the innovation of health monitoring systems, and the incorporation of verified drug testing into one's enhanced resume—illustrate that we are now living in a signaling world, in which firms can increasingly rely on information transmitted directly from a consumer to the firm instead of engaging in data mining to read the tea leaves about the consumer's characteristics or behavior.

The personal prospectus is a metaphor to represent the idea that signaling is becoming increasingly pervasive, cost-effective, and powerful as an economic mechanism. This section explores that evolution. Most fundamentally, this section makes an empirical claim: the Internet and digitization are decreasing the transaction costs of signaling by making verifiable signals more readily available throughout the economy, and one can therefore expect signaling to become more and more important and ubiquitous as a response to information asymmetries. This is a novel and somewhat radical claim. It sets the groundwork for Part II, which discusses the implications of these developments for informational privacy law.

I do not claim that signaling will eclipse sorting or that the digital dossier and the threat of sorting will become less important than the threats of signaling. I merely argue that signaling is increasing as signaling costs de-

---

[61] *See, e.g.*, SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY (2000) (discussing the threat of linked databases and the digitization of records); Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 435–36 (2008) (discussing the end of "practical obscurity" brought about by data mining); Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 291 (2003) ("[T]hree major digital developments . . . deeply affect privacy: (1) the increase in data creation and the resulting collection of vast amounts of personal data—caused by the recording of almost every modern interaction; (2) the globalization of the data market and the ability of anyone to collate and examine this data; and (3) lack of the types of control mechanisms for digital data that existed to protect analog data."); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 317–20 (2008) (discussing widespread use of data mining by government agencies and the government's reliance on commercial data gathering companies); Herman T. Tavani, *Informational Privacy, Data Mining, and the Internet*, 1 ETHICS & INFO. TECH. 137 (1999) (discussing the ethical implications of disclosure and data mining); Tal Z. Zarsky, *"Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE J.L. & TECH. 1 (2003) (discussing privacy concerns related to data mining); Jonathan Zittrain, *Privacy 2.0*, 2008 U. CHI. LEGAL F. 65, 77–86 (discussing various types of personal information now available digitally, including images and video); Seth Safier, *Between Big Brother and the Bottom Line: Privacy in Cyberspace*, 5 VA. J.L. & TECH. 6, at para. 10 (2000), http://www.vjolt.net/vol5/issue2/v5i2a6-Safier.html (discussing how these technologies allow for collection of "vast amounts of in-depth, and potentially sensitive, personal information").

crease and that this trend will change our understanding of informational privacy.

The key change causing the shift to the signaling economy is that digital information can be verified at very low cost. This change is occurring in at least two domains: *digital monitoring* of directly observable data and *digital access* to directly verifiable data. By "directly observable data" I mean the aggregated records from the many digital sensors monitoring one's life: the "black box" in one's car, the health monitor on one's wrist, the smart grid monitors in one's home. By "directly verifiable data" I mean verified information from reliable sources, such as one's income level, educational background and achievements, mental and physical health history, deeded or titled assets, credit history, immigration status, insurance coverage, employment history, professional licenses and status, registered holdings of public securities or participation in securities filings, registered patents or trademarks, criminal record, civil legal history, bankruptcy records, birth certificate information, marriage and divorce records, child support payment history, or tax history. MyBackgroundCheck.com's resume enhancement through verified drug testing is an example.[62] In addition, one could imagine that over time certain types of social media-driven information could enter the personal prospectus: one's Klout score, eBay Feedback score, or reputational ranking on industry-specific rating sites or reputation aggregators.[63]

Both types of information comprise one's personal prospectus. Both can be powerful signals of one's type to other economic actors. Both are playing an increasingly important role in the evolution of a signaling economy.

1. Digital Monitoring of Directly Observable Data.—Monitoring and sensor technology is increasingly sophisticated and pervasive. The data collected by such sensors is often both extremely personal and extremely valuable as part of an individual's personal prospectus. We are now able to track, record, and share more and better information about ourselves, and the technologies that enable signaling are evolving rapidly. Consider three contexts in which digital monitoring is expanding the scope of the personal prospectus: health care, equipment tracking, and employee monitoring.[64]

---

[62] *See supra* notes 10–11 and accompanying text.

[63] For discussion of Klout scores, see *supra* note 12. For discussion of reputation aggregators, see Ric Merrifield, *The Rise of the Reputation Score*, BLOGGING INNOVATION (Sept. 1, 2010), http://www.business-strategy-innovation.com/wordpress/2010/09/the-rise-of-the-reputation-score.

[64] In addition to the monitoring technologies discussed here, I have excluded others for brevity. Smart grid technologies, for instance, offer many similar monitoring and signaling opportunities. *See* Patrick McDaniel & Stephen McLaughlin, *Security and Privacy Challenges in the Smart Grid*, IEEE SECURITY & PRIVACY, May/June 2009, at 75, 77 ("Energy use information stored at the meter and distributed thereafter acts as an information-rich side channel, exposing customer habits and behaviors."); Elias Leake Quinn, *Privacy and the New Energy Infrastructure* 4–5 (Ctr. for Energy & Envtl. Sec., Working Paper No. 09-001, 2008), *available at* http://ssrn.com/abstract=1370731.

Remote health monitoring, or "pervasive health care," is a hot technology now that ubiquitous Internet access has made constant, real-time sensors possible.[65] Such monitoring is touted as a means to improve care and reduce health care costs.[66] Remote monitoring systems can track calorie use,[67] blood glucose levels,[68] arrhythmia,[69] epilepsy,[70] stress,[71] and vital signs such as temperature, heart rate, and respiration.[72] Intel is developing a "magic carpet" for the elderly that tracks their movement in the home to gather data to prevent falls, a major component of health costs for seniors.[73] Newer systems are also being imagined to remotely monitor the condition of mental health patients and addicts. These systems track sleep patterns, weight, physical movement, vital signs, and medication compliance to produce alerts for worsening mental illness[74] or addiction relapse.[75]

Individuals will also be increasingly able to use such monitors to signal their health characteristics for economic gain. The foundations are already laid for such signaling. Experts are discussing "pervasive lifestyle incentive management" systems that could electronically transfer micropayments to reward a user's exercise or healthy eating.[76] Employers have already begun to incentivize employees to participate in wellness programs or to meet health goals for blood pressure, cholesterol levels, or weight.[77] Some em-

---

[65] *See generally* Varshney, *supra* note 9, at 115 ("Comprehensive health monitoring services would allow patients to be monitored at any time in any location." (emphasis omitted)).

[66] *See, e.g.*, Upkar Varshney, *A Framework for Supporting Emergency Messages in Wireless Patient Monitoring*, 45 DECISION SUPPORT SYS. 981, 981 (2008) ("[P]atient monitoring using wireless technologies is being considered as a solution to both improving the quality of healthcare and reducing the rate of increase for healthcare services.").

[67] *See* BODYMEDIA, http://www.bodymedia.com (last visited Jan. 30, 2012).

[68] *See* IDEAL LIFE, http://www.ideallifeonline.com/products/glucomanager (last visited Jan. 30, 2012).

[69] *See Corventis™—NUVANT*, CORVENTIS, http://www.corventis.com/US/nuvant.asp (last visited Jan. 30, 2012).

[70] *See* Mohammad Modarreszadeh & Robert N. Schmidt, *Wireless, 32-Channel, EEG and Epilepsy Monitoring System*, 19 INT'L CONF. IEEE ENGINEERING MED. & BIOLOGY SOC. 1157, 1157 (1997).

[71] *See* Emil Jovanov et al., *Stress Monitoring Using a Distributed Wireless Intelligent Sensor System*, IEEE ENGINEERING MED. & BIOLOGY MAG., May/June 2003, at 49, 49.

[72] *See* TOUMAZ, http://www.toumaz.com (last visited Oct. 21, 2011) (offering wireless technology that tracks vital signs in real time).

[73] *See* Clark, *supra* note 6.

[74] *See* Upkar Varshney, *A Framework for Wireless Monitoring of Mental Health Conditions*, 31 INT'L CONF. IEEE ENGINEERING MED. BIOLOGY SOC. 5219, 5220 (2009).

[75] *See* Doug Cantor, *Brilliant 10: Santosh Kumar, the Sensor Guru*, POPULAR SCI. (Nov. 16, 2010, 3:08 PM), http://www.popsci.com/science/article/2010-10/brilliant-10-santosh-kumar-sensor-guru (discussing AutoSense, a system to remotely monitor stress and self-destructive behaviors in addiction therapy).

[76] *See* Varshney, *supra* note 9, at 115.

[77] Safeway, for example, has a "Healthy Measures" program that offers reimbursement for meeting certain wellness targets. *See* Harald Schmidt, Kristin Voigt & Daniel Wikler, *Carrots, Sticks, and Health Care Reform—Problems with Wellness Incentives*, 362 NEW ENG. J. MED. E3(1), E3(2) (2010) (discussing Safeway's program).

ployers have tracked employees' smoking habits even when the employees are away from their place of work.[78] Some have fired employees who engage in behavior likely to raise the employer's health insurance costs.[79]

Most dramatically, Congress recently endorsed incentive-based health reform in the health care bill.[80] Although group health plans generally cannot discriminate based on health status, the PPACA permits employers to provide discounts, rebates, and rewards for those who participate in wellness initiatives.[81] If the reward applies merely for participation, there is no limit to its scope. If the reward requires a participant to achieve a certain health target, the reward must not be greater than thirty percent of the cost of the health plan's coverage.[82] This is an increase from the twenty-percent cap that was in place under previous regulations.[83] In addition, under the PPACA, the Secretary for Labor, Health, and Human Services has discretion to increase this cap to fifty percent.[84]

Given this foundation, it is easy to imagine why individuals or employees would use remote health monitoring systems to secure discounts. A health-conscious employee who carefully controls her diet and exercises regularly may see such discounts as a justified reward for healthy behavior.

Monitoring is changing other markets as well. For example, car rental agencies have begun to implement tracking technologies to monitor driving habits and car use. This has generated some controversy. Recently courts in Connecticut[85] and California[86] have expressed concerns about the use of speed monitoring devices and GPS tracking in rental cars. These cases have focused on the consumer protection aspects of the contracts at issue,

---

[78] *See* Jeremy W. Peters, *Company's Smoking Ban Means Off-Hours, Too*, N.Y. TIMES, Feb. 8, 2005, at C5.

[79] Jill Schachner Chanen, *The Boss Is Watching*, 94 A.B.A. J. 48, 50–51 (2008).

[80] The PPACA codifies the incentive regulations previously established under the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

[81] For an overview of these changes, see U.S. CHAMBER OF COMMERCE, CRITICAL EMPLOYER ISSUES IN THE PATIENT PROTECTION AND AFFORDABLE CARE ACT 29 (2010).

[82] 42 U.S.C. § 300gg-4(j)(3)(A) (2006); *see also* U.S. CHAMBER OF COMMERCE, *supra* note 81, at 29.

[83] U.S. CHAMBER OF COMMERCE, *supra* note 81, at 29.

[84] *Id.*

[85] In *American Car Rental, Inc. v. Commissioner of Consumer Protection*, Connecticut filed an administrative complaint against a car rental agency that charged a $150 fee each time a customer's rental vehicle exceeded seventy-nine miles per hour for more than two consecutive minutes. 869 A.2d 1198, 1201 (Conn. 2005). The rental agreement warned customers that the agency's cars were "GPS equipped" and that the $150 fee would apply, but it did not explain GPS technology or provide details about the workings of the fee. *Id.* at 1201–02. The court found that the practice violated the Connecticut Unfair Trade Practices Act as an unfair penalty clause rather than a legitimate liquidated damages provision. *Id.* at 1201.

[86] In *People v. Acceleron Corp.*, California alleged that the rental car company failed to inform consumers about the use of GPS tracking technology and the fee the company imposed if a consumer drove a car outside of California. *See* Complaint at 3, People v. Acceleron Corp., No. 04-129 (Cal. Super. Ct. Nov. 9, 2004), *available at* http://ag.ca.gov/newsalerts/cms04/04-129_complaint.pdf.

generally finding a failure to sufficiently notify consumers about the devices or fees. They have generally held that rental car companies "may use tracking technology . . . so long as companies clearly and conspicuously notify customers of such use."[87] In addition, at least three states[88] have enacted statutes restricting the use of such monitors.[89] California and New York, for example, strictly constrain the use of GPS or other tracking technology to gather information about a consumer's use of a rental car except to locate a stolen or missing vehicle.[90]

Note that, in each of these examples, the rental car agency imposed a punitive fee on the consumer for misuse of the vehicle. It is quite possible that had these "fees" for bad behavior instead been framed as "discounts" for good behavior, no consumer litigation would have resulted. No state has directly addressed the consumer's potential *interest* in sharing GPS-enabled information about her use of a rental vehicle to receive a discount. The car insurance examples[91] suggest that discount-based programs will fare better than fee-based penalties.

Location-enabled smart phone applications and services are increasingly turning to such discounts to incentivize location-revelation. For example, DailyCandy's Android phone application uses GPS location information to offer discounts on clothing and other merchandise to shoppers as they walk by participating shops.[92] Shopkick provides department stores, coffee shops, and shopping malls with devices that emit an inaudible sound detectable only by an iPhone or Android phone with the Shopkick application; shoppers browsing in a Best Buy, American Eagle Outfitters, Target, Macy's, or Sports Authority can then earn "kickbucks" simply for entering the store.[93] Kickbucks are redeemable for prizes—including downloadable songs and donations to charity—as well as in-store discounts that

---

[87] *See* Leah Altaras, *Follow that Car! Legal Issues Arising from Installation of Tracking Devices in Leased Consumer Goods and Equipment*, 3 SHIDLER J.L. COM. & TECH. 8, at para. 16 (2007).

[88] *See* CAL. CIV. CODE § 1936(o) (West 2010); CONN. GEN. STAT. ANN. § 42a-9-609 (West 2010); N.Y. GEN. BUS. LAW § 396-z(13-a) (McKinney 2011).

[89] States have similarly regulated the use of GPS or other tracking technologies in privately owned vehicles. Such statutes generally require manufacturers to disclose the presence of such technology to a car buyer. In addition, various states have required the consumer's consent to access data created by such devices. No states, however, have banned such devices or banned consumers from disclosing such information as they see fit. *See* Altaras, *supra* note 87, at 22–30 (discussing state legislation).

[90] CAL. CIV. CODE § 1936(o); N.Y. GEN. BUS. LAW § 396-z(13-a).

[91] *See supra* notes 1–4.

[92] *See Stylish NYC Alerts on Your Android Phone*, DAILY CANDY (Aug. 4, 2010), http://www.dailycandy.com/all-cities/article/85902/Stylish-NYC-Alerts-on-Your-Android-Phone.

[93] *See* SHOPKICK, http://www.shopkick.com (last visited Jan. 30, 2012); Tom Simonite, *Bringing Cell-Phone Location-Sensing Indoors*, TECH. REV. (Aug. 31, 2010), http://www.technologyreview.com/communications/26156/. Other companies are also working to pinpoint a consumer's location inside a given store or mall. *See, e.g.*, POINT INSIDE, http://www.pointinside.com (last visited Jan. 30, 2012).

ring up at the cash register automatically.[94] Finally, the discounts offered by "check-in" location services such as FourSquare[95] and Facebook[96] further suggest that incentives may persuade users to disclose such data.[97]

Next consider employee monitoring. Employers have always sought more and better information about employees' whereabouts, effort, and output. Digital monitoring increasingly allows employees to signal the quality of their work and trustworthiness to their employers by revealing private personal information.

In some cases, employees have been asked to consent to tracking in return for some offered benefit. In *Department of Education v. Halpin*, for example, an employee was terminated after GPS technology in an employer-issued cell phone revealed that he had misrepresented his whereabouts on his time records.[98] The administrative court noted that the employee had not been required to use the cell phone; other employees refused the offered phones. The employee in question accepted the benefit of the phone and with it the employer's tracking technology.[99]

Such employee tracking will likely increase if radio frequency identification (RFID) becomes more ubiquitous. Although RFID adoption has been slower than many originally predicted, RFID tags have been used to track employees as they move around various settings.[100] The Dubai International Airport uses RFID tags to track over 9000 workers, the security firm CityWatcher is experimenting with subcutaneous RFID tags implanted into the forearms of some employees as a security measure, and the Oak Ridge National Laboratories in Tennessee uses RFID to monitor whether employees have properly evacuated in emergency situations.[101]

---

[94] *See The App*, SHOPKICK, http://www.shopkick.com/app.html (last visited Jan. 30, 2012); *see also* Simonite, *supra* note 93 (describing the technology behind Shopkick).

[95] *See* FOURSQUARE, http://www.foursquare.com (last visited Jan. 30, 2012).

[96] *See Share Where You Are*, FACEBOOK, http://www.facebook.com/about/location (last visited Oct. 21, 2011) (formerly known as Facebook Places).

[97] *See* Andrew Weinreich, *Check-ins vs. Persistent Location: How Big a Deal Is Facebook Places?*, HUFFINGTON POST (Aug. 31, 2010, 3:24 PM), http://www.huffingtonpost.com/andrew-weinreich/checkins-vs-persistent-lo_1_b_699653.html (arguing that widespread location disclosure "will only happen when the user believes the value derived from the service outweighs any perceived privacy risks from sharing his location" and that "[f]or persistent location to work . . . I have to be motivated by cheap lattes").

[98] OATH Index No. 818/07, 2 (N.Y.C. Office of Admin. Trials & Hearings Aug. 9, 2007).

[99] For additional discussion, see *NoviTech Now Using Active RFID System for Employee Monitoring*, RFIDNEWS (Aug. 28, 2007), http://www.rfidnews.org/2007/08/28/novitech-now-using-active-rfid-system-for-employee-monitoring.

[100] *See id.*; *Real Time Employee Tracking Helps Home Caregivers*, CONTACTLESSNEWS (Feb. 4, 2008), http://www.contactlessnews.com/2008/02/04/real-time-employee-tracking-helps-home-caregivers.

[101] These examples are drawn from Marisa Anne Pagnattaro, *Getting Under Your Skin—Literally: RFID in the Employment Context*, 2008 U. ILL. J.L. TECH. & POL'Y 237, 242–43.

The privacy aspects of RFID have received some attention in the legal literature,[102] and several states have prohibited employers from requiring employees to implant subcutaneous RFID tags.[103] No state, however, has forbidden employees from consenting to such tracking. Employees willing to accept tracking technologies such as GPS or RFID to signal their loyalty, diligence, or cooperation are therefore able to do so to distinguish themselves from their peers.[104]

Regardless of its context—health, equipment rental, or employment—this directly observable data divides into three basic types. First, some of these technologies allow an uninformed economic counterparty direct access to the information it wants. Thus, for example, a health insurer or employer might want to know whether an individual is exercising. If the individual's heart rate or miles walked per day can be monitored directly, the uninformed counterparty becomes directly informed.[105] The previously uninformed counterparty does not need to sort based on proxies for exercise such as education level or geographical location, nor does the individual signal her type exactly. She is merely providing direct data about her type to the previously uninformed party.

Second, in many instances the exact trait in question cannot be directly monitored even with advanced digital sensors. An employer might care most about an employee's diligence or persistence, but no digital sensor can directly reveal such characteristics. An employee might consent to an RFID badge or other monitors of his whereabouts, however, to reveal the amount of time spent at his desk, as opposed to the water cooler, hoping that this proxy for persistence or diligence would impress his employer. Many of the economic uses for these digital sensors are of this type: they provide new proxies for traits that are otherwise difficult to monitor.

Third, an individual's willingness to be monitored may *in itself* be a signal of certain desirable qualities. The Tiwi system, for example, is a monitoring device meant to improve teenage driving. It allows parents to see the location of their teenager's car, receive instant alerts if their teenager is speeding, and know whether their teenager's seat belt is buckled.[106] The

---

[102] *See, e.g.*, Kyle Sommer, *Riding the Wave: The Uncertain Future of RFID Legislation*, 35 J. LEGIS. 48 (2009); Jonathan Weinberg, *Tracking RFID*, 3 I/S J.L. & POL'Y INFO. SOC'Y 777 (2008); Reuven R. Levary et al., *Radio Frequency Identification: Legal Aspects*, RICH. J.L. & TECH., Fall 2005, at 1, 3–6, http://jolt.richmond.edu/v12i2/article6.pdf; Serena G. Stein, *Where Will Consumers Find Privacy Protection from RFIDs?: A Case for Federal Legislation*, DUKE L. & TECH. REV. (Mar. 8, 2007), http://www.law.duke.edu/journals/dltr/articles/2007DLTR0003.html.

[103] No federal statutes expressly relate to RFID. Some states have regulated RFID's use or forbidden requiring employees to implant subcutaneous RFID chips. *See* Pagnattaro, *supra* note 101, at 247–49 (reviewing state statutes).

[104] *See id.* at 248 (raising the question of "voluntary" adoption of RFID or GPS disclosure in passing but without discussion).

[105] This technology exists. *See* FITBIT, *supra* note 8.

[106] *See The Features*, TIWI, http://www.tiwi.com/for_families/the_features (last visited Jan. 30, 2012).

AnPac Insurance Company's DriveSmart program currently offers discounts for teens using Tiwi.[107] DriveSmart differs, however, from the car insurance monitoring programs already discussed. Unlike programs in which the insurance carrier receives the monitored data, and such information directly affects the insured's premiums, DriveSmart does not receive the collected information. Instead, AnPac offers a discount merely because the teenager's *parents* are receiving the data, which signals to AnPac that the teenager and her parents are responsible and care about driving safety.[108]

Regardless of whether sensor technology provides direct observation of an economically desired trait, the ability to signal a desired trait, or the ability to indirectly signal one's type merely by using the technology, such monitoring is already vastly increasing the amount and quality of information a person can share about herself. It is a key component of the personal prospectus: a huge pool of verified, high-quality information that an individual can make available to others for economic purposes.

2. Digital Access to Directly Verifiable Data.—Direct digital monitoring is one source of information for the personal prospectus, but it is not, and will not be, the only source. Instead, a second type of information may come to be at least as important: information individuals choose to share by granting digital access to directly verifiable personal data.

Currently each of us has access to many different databases containing our personal information.[109] I may have a bank account at Chase Bank, an investment account at Charles Schwab, an individual retirement account at Fidelity, and an online repository for my medical records on Google Health. In addition, many important facts about us are kept in digital databases to which we do not have immediate access, but could. For example, the university from which I graduated holds my educational records and achievements; my employer holds my employment history, salary, and evaluations; the government holds my tax records; and the court system holds documentation of my criminal and legal history.

As information technologies advance, it will be easier and easier to share such information about oneself by granting others temporary permission to query one's personal records. In other words, consumers will be able to digitally link an interested counterparty to these sources that hold

---

[107] *See Parents Help Keep Teen Drivers Safe with DriveSmart*, *supra* note 4.

[108] *See id.*

[109] Although the Internet era has vastly increased the aggregated information available to data miners, this sea of information has filled in around the islands of more secure, more personal information that continue to remain largely under individual control (e.g., bank account or investment information). I call these islands the "private remainder." There are generally five categories of such information: financial information (including tax records), medical information, educational information, employment information (including the regulation of background checks), and library and video rental information. For an excellent overview of the various privacy statutes and regulations, see Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 359–62, 364–68, which summarizes the Fair Credit Reporting Act, the Privacy Act, and the limits of U.S. privacy law.

verified evidence about themselves. If applying for a loan, one will not merely disclose "I make $100,000 per year" but will instead point the potential lender to the source of the information on which those words are based—in this case, to the employer who pays the $100,000 salary. The borrower will digitally link a potential lender to the borrower's employer and give the lender instant access to the employer's verified salary information.[110] Your employer's computer will simply issue a verification of the requested information: "Yes, she does indeed make $100,000."

In addition to a resume, individuals will grant access to their personal prospectus and the underlying verified data to which a resume typically attests. Employment history will be verified as employers, or the Internal Revenue Service, share data in response to authorized queries about an individual's work record. Criminal history will be verified as court clerks share data in response to authorized queries about an individual's past. Medical records will be verified as physicians, hospitals, and insurance companies share data in response to authorized queries about an individual's medical history. Immigration status, professional licenses, military records, tax compliance history, and other data will be verified through government data sources.

Connected to the raw, verified data in this way, the personal prospectus becomes an even more powerful signaling tool than if it only contained the digital record from direct monitoring devices. As the economy's information architecture makes digital records increasingly portable, comparable, and verifiable, an individual will be able to present himself to others through the personal prospectus—to show his type, characteristics, and history by revealing verified information about himself.

The personal prospectus would thus differ from the digital dossier in two primary ways.[111] First, the prospectus would be comprised of *verified* information whereas the digital dossier is largely comprised of unverified

---

[110] Since the invention of hypertext, there has been discussion of the extent to which web information should be linked back to its source. Ted Nelson, the man who coined the term "hypertext," originally envisioned that all *text* on the web would be linked to its originating source, so that use of the text could be controlled by its original author and micropayments could be made for "downstream" use of the text. Discussion continues about the extent to which web text, images, and other information can and should be linked to its source. *See generally* Zittrain, *supra* note 61, at 107–08 (discussing Nelson's original vision and the current debate on the issue). The personal prospectus is a related idea. Rather than focus on authorial content shared over the web such as a book or photograph, I focus on data about a person that originally reside in an institution's database but are then released onto the web and wind up in the digital dossier.

[111] There is a third way that it differs from the digital dossier: constraining moral hazard. In the Introduction, Tom Goodwin notes that having a monitor in his car makes him drive more carefully. This is an advantage of the personal prospectus—or disclosure—over the digital dossier. When an insurance company sorts insureds without their knowledge using the digital dossier, the insurance company reaps no benefit in terms of constraining moral hazard. When an insured agrees to disclose their information through the personal prospectus, by contrast, they are aware of that disclosure and are more likely to regulate their behavior in the future.

information. The prospectus would be made up of information that was tied back, digitally, to its source. For example, the prospectus would not just contain a copy of a medical record—it would contain the copy *and* a digital signature certifying the record as legitimate and linking that record back to the physician or hospital that originally issued it. The prospectus would contain not only an educational transcript but also a digital connection to the university or graduate school from which the student graduated. It would, in short, be a verified database of information about the individual—not just the individual's representation of herself but the individual's collection of others' certified records about her. This increases the signaling value of the data tremendously.

Second, even the public information in the personal prospectus would be different in kind from the information in the digital dossier. Whereas the digital dossier might contain information about one's criminal record or professional licenses, that information is unverified—when one runs a background check on someone using the public information available on the Internet, there is no guarantee that the right information has been pulled on the right individual nor that the information is accurate. If an individual electronically compiled a personal prospectus over the course of her lifetime, however, such information would be included in a verified form. This would make such public information in the personal prospectus more valuable than the "same" piece of information in the digital dossier.

To illustrate, contrast what might be in a hypothetical "John Smith's" digital dossier with what might be in his personal prospectus. Today, one could run a credit search, criminal background check, or Google search on John Smith and find the scattered pieces of his digital dossier. One might turn up the addresses John has resided at in the last few years or the companies he has worked for. One might discover that his credit rating is not the best or that he has a history of traffic violations. All of these pieces of information could be aggregated from John's digital dossier to form a picture of John and to sort John from other potential economic counterparts.

In the future, however, John might have a digital personal prospectus available with verified information about himself. He could make that prospectus available to signal his qualities and characteristics. One could query that data set to find his court or criminal record directly. His traffic violations would appear but so would the community service he did to clear his record. The name of his employers would appear but so would the personnel records that John chose to disclose: his record of promotions, salary levels, or relevant parts of his performance reports. John's residences would appear but so would the record of his rent payments from each landlord or even the landlord's assessments of John as a tenant. And importantly, the person searching for this information would be confident (or at least more confident) that the search results were actually about the *right* John Smith. Rather than search the digital dossier and receive results of

questionable value, an employer or landlord could simply get the information from John directly.

This is the power of the personal prospectus: to proactively assert one's identity into the economy rather than having to react to the sea of information in the digital dossier, into which one has little visibility and over which one has little control.[112] If John were a good credit risk, he could assert that fact by granting potential lenders temporary access to records of other loans outstanding and his payment histories on those loans. He could reveal his credit card transactions for the last three years, showing his record of paying his balance on time and spending responsibly. He could signal his strength as a borrower by showing his reliability as an employee, revealing to a lender his employment history. John's personal prospectus could offer him the chance to proactively signal his qualities.

II. SIGNALING'S UNRAVELING THREAT TO INFORMATIONAL PRIVACY

The personal prospectus promises the ability to proactively assert oneself in the economy. That promise, however, contains within it a radical threat: the possible unraveling of privacy altogether because some individuals initially will find it in their interest to disclose information for personal gain and then, as the unraveling proceeds, everyone will realize that disclosure is no longer a choice because the signaling economy attaches stigma to staying silent.

This Part explores this unraveling effect, a phenomenon discussed by law and economics scholars since the early 1980s in other contexts but not taken up generally by privacy scholars. It argues that the arrival of the personal prospectus and a signaling economy should bring the unraveling problem to the fore of informational privacy discussion.

A. Unraveling in a Signaling Economy

As low-cost signaling evolves and becomes more ubiquitous, the first and most fundamental point is that some people will want to disclose and others will not. Everyone may eventually discover, however, that they have little choice. At first, those with positive private information (the "top" of the pool) will disclose to seek discounts and economic benefit and to defend against the negative effects of the digital dossier. Eventually, even those with the worst private information (the "bottom" of the pool) may realize that they have little choice but to disclose to avoid the stigma of keeping information secret. A given individual might benefit by signaling in one context (e.g., good drivers will seek cheaper car insurance), but few people if

[112] A few firms are experimenting with business models that seem very much like the idea of the personal prospectus. *See* ALLOW, http://www.i-allow.com (last visited Jan. 30, 2012); PERSONAL, http://www.personal.com (last visited Jan. 30, 2012). For further analysis of these recent startups, see Scott R. Peppet, Privacy Intermediaries (work in progress) (on file with author).

any will gain in every context. As signaling becomes more pervasive, however, disclosure may become the norm across the economy. Keeping one's personal prospectus private may become suspect. This is the unraveling threat to privacy.

1. Self-interested Self-disclosure and Defending Against the Digital Dossier.—Simple self-interest will drive self-disclosure by those with favorable private information. Assuming one has positive characteristics to share, revealing them can provide economic benefits.[113] This is what the car insurance, health monitoring, and employment tracking examples illustrate: in markets with information asymmetry, individuals will seek preferential treatment or discounts in return for disclosing information useful to other economic actors.

Although most privacy literature has focused on how individuals can and should keep their information to ourselves, it ignores the reality that in many cases it is extremely valuable to share information about oneself with others.[114] The privacy field has been so concerned with the downsides of sorting that it has sometimes overlooked that many people will, at least initially, reap benefits from increased signaling.[115] For a healthy, nonsmoking, regular exerciser, a means to credibly signal that information to one's medical insurer will mean lower premiums. For a dependable, income-earning employee, a means to credibly signal that information to one's bank will mean lower rates. For a customer with a large bank account and a string of other assets, a means to credibly signal that information to a luxury store will mean better service.[116]

Signaling through the personal prospectus will also counter the negative effects of the digital dossier. As discussed, one of the threats of the dossier is inaccurate representation in the economy. Even if someone is a "good" borrower or a low-risk insured, the digital dossier may still incorrectly sort her into the wrong category. Signaling via the personal prospectus can correct the inaccuracies of the dossier. To see how, consider some

---

[113] I do not mean to reduce privacy's value to purely economic terms. For those with favorable personal information, self-disclosure may also be dignity-enhancing as an expressive or self-affirming act. *See generally* Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962 (1964); Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1832–33 (2010) (discussing dignity-enhancing aspects of privacy).

[114] *See* Stan Karas, *Loving Big Brother*, 15 ALB. L.J. SCI. & TECH. 607, 626 (2005) (arguing that there are certain circumstances in which a person benefits by disclosing information to others).

[115] I should acknowledge the work of privacy scholars who have highlighted the value of privacy losses. *See, e.g.*, DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998); FRED H. CATE, PRIVACY IN PERSPECTIVE (2001); Lior Jacob Strahilevitz, *Reputation Nation: Law in an Era of Ubiquitous Personal Information*, 102 NW. U. L. REV. 1667, 1676 (2008).

[116] *See* Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1049–50 (1999) (discussing the ways in which self-disclosure can reduce search costs).

of the core concerns that privacy scholars have raised about the spread and use of the digital dossier. In each instance, signaling through disclosure of the personal prospectus offers a potential counter to the problems of the digital dossier.

The first concern about the digital dossier is that it oversimplifies the individual.[117] The digital dossier reduces the inherent complexity of an individual's identity. Instead of being individualized and context-sensitive, computerized sorting is lumpy: it classifies people together based on measurable characteristics that do not necessarily accurately represent any given individual.[118] We are not just sorted; an *abstraction* of us is sorted, assessed, categorized, and acted upon.[119]

The prospectus offers the individual the ability to represent *herself* instead of being passively represented by the dossier. By sharing information proactively instead of reacting to the sorting mechanisms, the individual regains influence over her life. At least initially, she can choose whether and what to share. This offers the possibility of a richer, more complete self-portrayal.

The second fear of the dossier is its inherent risk of inaccuracy. There are many potential sources for inaccuracies in the digital dossier. At the most mundane, online digital information may contain errors because of incorrect entry, aggregation,[120] or data retrieval.[121] Twenty-five percent of credit reports contain serious errors, and roughly fifty percent contain inaccurate or outdated information.[122] They may contain information about

---

[117] *See* SOLOVE, *supra* note 17, at 46.

[118] *See* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 115 (2000) ("Privacy . . . protects us from being objectified and simplified and judged out of context in a world of short attention spans, a world in which part of our identity can be mistaken for the whole of our identity."); *see also* JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE (2004) (discussing privacy and security technology in a post-9/11 era).

[119] *See* Elia Zureik, *Theorizing Surveillance: The Case of the Workplace*, *in* SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK, AND DIGITAL DISCRIMINATION 31, 39 (David Lyon ed., 2003) ("As a matter of fact, the subject that is exposed to the 'observing gaze' dissolves and is reconstituted in the abstract through categorization and social ordering . . . ."). *But see* Karas, *supra* note 114, at 627–28 ("[F]or some, submission to surveillance may enable a sharper, more stable sense of self.").

This concern is not new. For a discussion of historical concern about the "invention of disembodied financial identity" in the nineteenth century, see Lauer, *supra* note 44, at 302.

[120] Ramasastry, *supra* note 57, at 757–60 (arguing that a "giant game of telephone is going on with our personal data" and discussing how different the final information in a dossier can be from how it began).

[121] *See* Kim Zetter, *Bad Data Fouls Background Checks*, WIRED (Mar. 11, 2005), http://www.wired.com/politics/security/news/2005/03/66856 (discussing problems of error-filled databases).

[122] Slobogin, *supra* note 61, at 324 (stating that one in four credit reports contain serious enough errors to deny credit, employment, or housing, and that fifty-four percent contain outdated or otherwise inaccurate information or information about other people); *see* Elizabeth D. De Armond, *Frothy Chaos: Modern Data Warehousing and Old-Fashioned Defamation*, 41 VAL. U. L. REV. 1061, 1076 (2007) (stating that nearly eighty percent of credit reports contain errors); Zetter, *supra* note 121 (stating that seventy-nine percent of credit reports contain errors).

another person altogether, particularly when one has a common name like John Smith.[123] In short, the digital dossier is noisy.

The personal prospectus offers obvious advantages over the dossier on this score. If an individual can aggregate verified information about herself to share with others, the individual knows that the information is accurate and that it is indeed *her* information.[124] This, again, empowers the individual to assert herself in the world by portraying herself accurately.

The third objection to the dossier is that one has no recourse against it.[125] There is no phone number to call to inspect one's digital dossier and no website to check. Instead, one is being represented by a vague cloud of information that one cannot control. The prospectus, in contrast, can be reviewed. Although an individual could not necessarily *change* the information in her prospectus, she would at least know what information it contained.[126]

Finally, the fourth and most fundamental concern is *discrimination*. As we have seen, sorting is the essential function of the digital dossier, and thus the dossier threatens to spawn new forms of unwanted discrimination. Consider a local bank trying to determine how to serve two customers, Alice and Bob.[127] Through its data mining efforts, the bank determines that Alice is a likely high-value customer whereas Bob is not. And Alice is likely to be susceptible to offers from other banks that would pull her away whereas Bob is not. The local bank decides to offer Alice an attractive interest-bearing checking account and a reduced loan rate to induce her to stay loyal. Bob, on the other hand, receives no such benefits and may even be burdened with higher fees and other measures meant to induce him to

---

[123] *See* De Armond, *supra* note 122, at 1075 ("A certain amount of information attributed to any one individual may be false.").

[124] Although the personal prospectus offers the individual the ability to represent herself accurately to others, it also introduces the possibility of misrepresentation. I assume here that the personal prospectus is verified by tying its contents digitally to their sources. There is some possibility, of course, of individuals attempting to hack this process to falsify their personal records.

[125] *See* Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 576–84 (2008) (discussing benefits and risks of the spread of digital dossiers, including the lack of real verification or recourse); *see also* SOLOVE, *supra* note 17, at 96 ("[T]he growing use and dissemination of personal information creates a Kafkaesque world of bureaucracy, where we are increasingly powerless and vulnerable, where personal information is not only outside our control but also is subjected to a bureaucratic process that is itself not adequately controlled.").

[126] Because the information within a personal prospectus would be *verified* information linked back to its source for easy verification, an individual could not simply enter the prospectus and edit the information.

[127] This example is drawn from Anthony Danna & Oscar H. Gandy, Jr., *All That Glitters Is Not Gold: Digging Beneath the Surface of Data Mining*, 40 J. BUS. ETHICS 373, 375 (2002).

take his business elsewhere. Some have labeled this "weblining" to evoke the pejorative connotations of "redlining."[128]

The personal prospectus would not so much counter economic discrimination as make it more accurate—more fair, so to speak, if not more just. The increased accuracy of the information in the personal prospectus would allow an individual consumer to ensure that she was sorted properly—if she had to be sorted. In other words, by signaling, individuals could ensure that they were treated according to their *actual* characteristics, not according to the potentially inaccurate caricature found in the digital dossier.[129]

This may be small consolation, but it is likely to be the reality of a signaling economy. In an economy with robust signaling, those with strong reputations, valuable credentials, clean medical records, impressive credit scores, and big pocketbooks will *want* to signal those characteristics in hopes of receiving preferential treatment by other economic actors.

2. Stigma and Unraveling.—Now we come to the heart of the matter. In addition to these self-interested reasons for availing oneself of the personal prospectus, a different motivation for self-disclosure may creep into the economy as well. As the personal prospectus becomes more accepted, it will give rise to its own stigma: when disclosure becomes low-cost and routine, those who hold out are suspect. This is the privacy threat of the personal prospectus. Failure to make one's personal prospectus available to the bank, the credit card company, the insurance agent, or the potential employer may carry with it the presumption that one is hiding information. You can be sorted *because* you do not signal.

This is the core insight of the unraveling effect in economics. Early work by Paul Milgrom[130] and Sanford Grossman[131] independently explored the unraveling process that occurs as those who can certify their quality do so to distinguish themselves from the larger pool of lower-grade labor,

---

[128] *See* David Lyon, *Surveillance as Social Sorting: Computer Codes and Mobile Bodies*, *in* SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK, AND DIGITAL DISCRIMINATION, *supra* note 119, at 13, 14 ("In processes known variously as 'digital redlining' or 'weblining', customers are classified according to their relative worth." (citations omitted)); Janet Dean Gertz, Comment, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943, 961 (2002) ("[P]rofiling may simply be a new and insidious legal form of discrimination that merely automates old-fashioned redlining practices.").

[129] *See* Strahilevitz, *supra* note 115, at 1676 ("Often, the choice is not between sorting and not sorting; the economic and social gains from sorting are simply too great, while banning sorting in many contexts will be simultaneously costly and not terribly effective. Rather, the real choice is between sorting on the basis of uncomfortable criteria and sorting on the basis of obnoxious and distasteful criteria.").

[130] *See* Paul R. Milgrom, *Good News and Bad News: Representation Theorems and Applications*, 12 BELL J. ECON. 380, 388 (1981) (discussing the salesman's incentive to fully disclose product quality because of similar unraveling effect).

[131] *See* Sanford J. Grossman, *The Informational Role of Warranties and Private Disclosure About Product Quality*, 24 J.L. & ECON. 461 (1981); Grossman & Hart, *supra* note 14, at 323 ("[I]f there is no transactions cost then it will always be in the seller's interest to disclose the quality of [an] item voluntarily.").

products, or services.[132] Others have followed in these footsteps, exploring the unraveling of information under various conditions (competitive versus monopolistic markets, etc.) and in various contexts (disclosure of product quality, securities-related information, pretrial settlement, etc.).[133]

The unraveling effect holds that under conditions of information asymmetry but with verifiable information and penalties for fraud,[134] every member of a pool will ultimately reveal its type even if at first it seems unwise for each to do so. At first the individual with the "best" trait has reason to disclose her type because her trait is better than the average; being lumped together with the rest of the pool is not in her self-interest. Once the best individual has disclosed her type, however, the "average" type remaining in the pool shifts. Now the second-best individual has a similar interest in disclosure. The average quality drops again. As Robert Frank puts it, "The unraveling process is set in motion, and in the end all [individuals] must either [disclose] or live with the knowledge" that others will assume they are of the "worst" type.[135] "The general message of the full-disclosure principle is that lack of evidence that something resides in a favored category will often suggest that it belongs to a less favored one."[136]

In a signaling economy, consumers may increasingly pay a price for keeping personal information private. Paying the price of not signaling differs from price discrimination or weblining because in the latter instances a firm is sorting a consumer based on the consumer's known (or supposed) characteristics derived from information about that consumer in the digital dossier. But here the firm need not even inspect the consumer's digital dossier: the firm will assume that it has learned something about the consumer merely by being denied access to the consumer's personal prospectus.

---

[132] Although Grossman and Milgrom are generally credited with the effect, Kip Viscusi first used the term "unraveling." *See* W. Kip Viscusi, *A Note on "Lemons" Markets with Quality Certification*, 9 BELL J. ECON. 277, 278 (1978) ("[E]nterprises or individuals at the above-average end of the quality spectrum successively distinguish themselves from the group in a process that unravels from the top down."); *see also* W. KIP VISCUSI, RISK BY CHOICE 86 (1983) (discussing unraveling).

[133] *See, e.g.*, Ronald A. Dye & Sri S. Sridhar, *Industry-Wide Disclosure Dynamics*, 33 J. ACCT. RES. 157, 157 (1995) (looking at unraveling across an industry as "[v]oluntary disclosures by some firms . . . provoke other firms to make related disclosures"); Joseph Farrell, *Voluntary Disclosure: Robustness of the Unraveling Result, and Comments on Its Importance*, *in* ANTITRUST AND REGULATION 91 (Ronald E. Grieson, ed., 1986); Andrew E. Stivers, *Unraveling of Information: Competition and Uncertainty*, 4 TOPICS THEORETICAL ECON. 1 (2004) (finding that increased competition in market increases unraveling effect). For early work on pretrial settlement, see Steven Shavell, *Sharing of Information Prior to Settlement or Litigation*, 20 RAND J. ECON. 183 (1989).

[134] There do not necessarily need to be formal or legal sanctions for misrepresentation. *See* Trevon Logan & Manisha Shah, *Face Value: Information and Signaling in an Illegal Market* (Nat'l Bureau of Econ. Research, Working Paper No. 14841, 2009), *available at* http://ssrn.com/abstract=1376153 (demonstrating that male sex workers disclose face pictures readily and accurately, and that unraveling is sufficiently supported by informal enforcement mechanisms to overcome adverse selection).

[135] FRANK, *supra* note 16, at 106.

[136] *Id.* at 106–08.

Return again to some of the examples considered thus far. If one can cost-effectively monitor an employee's exercise habits with a digital armband, what would prevent an employer from drawing negative inferences about employees who refuse such devices? If one can easily verify whether a diabetic, heart patient, or psychiatric patient is regulating her blood sugar, heart rate, or medications properly, why would an insurer not draw negative inferences from patients refusing to participate in a discount program aimed at incentivizing such responsible behaviors? To put a point on it, how suspect would you look if your significant other or spouse asked you to join him or her in signing up for mutual location-tracking via smart phone, and you refused?[137] Once sharing such information becomes cost-effective, not sharing such information may begin to require justification.

B. Informational Privacy Law's Unpreparedness for Unraveling

I do not pretend to be the first to consider the threat of unraveling in the privacy context. I believe Judge Richard Posner should claim that title, and a few others have since taken up his connection between unraveling and privacy.[138] As Posner put it,

> Because people who are above average in any valued attribute have an incentive to signal their possession of that attribute, the existence of discrediting information about persons is likely to become known even if the law does protect such information, unless disclosure is costly for reasons unrelated to the private benefits of concealment or the signal is easily faked.[139]

To date, however, privacy scholars, including Posner, have not treated the unraveling of privacy as a practical problem so much as a theoretical novelty. Happily for privacy advocates, there *has* been a "reason[] unrelated to the private benefits of concealment" that has prevented unraveling to date: the lack of technological means to build a robust signaling economy. It has

---

[137] Such applications already exist. Most request permission before disclosing your location to another smart phone user. *See, e.g.*, *GPS Tracking App–iLOCi2 for iPhone*, LOCIMOBILE, http://www.locimobile.com/iloci2 (last visited Jan. 30, 2012). Some can be installed surreptitiously on a smart phone to track that phone without the user's knowledge. *See, e.g.*, MOBILE SPY, http://www.mobilespytool.com (last visited Jan. 30, 2012).

[138] Jessica Litman's early article on privacy as a property right saw the unraveling problem, for example. *See* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000). She notes that control is at best a stepping stone towards alienability. *See id.* at 1300. Most interesting, Litman hints at unraveling: "If easy assignment is the rule, they may no longer have the power to preserve their secrecy; even if they could, the exceptional nature of their asserting a privacy claim will tip off those from whom this is a secret that there is an interesting secret there." *Id.* at 1301; *see also* Randal C. Picker, *Online Advertising, Identity and Privacy* (Univ. of Chi., John M. Olin Law & Econ., Working Paper No. 475, 2009), *available at* http://www.law.uchicago.edu/files/files/475.rcp_.online.pdf (discussing unraveling in the context of smoking and revelation of behavioral preferences, and talking about the "privacy externalities" created when one person reveals information that begins an unraveling that forces others to reveal).

[139] POSNER, *supra* note †, at 107.

been cheaper to mine for data than to rely on signals. But that is changing. The costs of signaling are dropping, just as the costs of data mining and sorting have dropped. Although the Internet-based monitoring and information-sharing technologies so central to the personal prospectus did not exist when Posner first discussed unraveling, they now make the personal prospectus a real possibility and a real threat to personal privacy.

Unraveling suggests two sweeping critiques of the dominant approaches to informational privacy. First, when it comes to prescriptions—what to do next—informational privacy scholarship has almost exclusively proposed solutions that seek to increase individual control over information. Control, however, provides little protection from unraveling. Second, and more fundamentally, the field has defined what constitutes a privacy harm too narrowly. It has assumed that voluntary disclosure causes no privacy problem, an assumption that the threat of unraveling complicates dramatically. Let us consider each problem in turn.

1. The Inadequacy of Control.—Space and attention span do not permit an exhaustive overview of the voluminous literature produced by informational privacy scholars over the last two decades. Nor do I want to be overly reductionist in describing the privacy field, which is rich and varied. For example, recent work has exploded the definitions of what constitutes "privacy,"[140] as well as begun to reimagine what constitutes privacy harm.[141] Both exercises are laudable and useful.

But even a cursory review of the privacy literature should suffice to demonstrate that control dominates as the primary solution of privacy advocates.[142] For example, much informational privacy literature has focused on property-based prescriptions. The basic idea is this: "[P]rivacy can be cast as a property right. People should *own* information about themselves and, as owners of property, should be entitled to control what is done with it."[143] As Arthur Miller put it in his early privacy work, "If this premise is accepted, the natural corollary is that a [person] has the right to control information about himself and is eligible for the full range of legal protection

---

[140] *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 101–70 (2008) [hereinafter SOLOVE, UNDERSTANDING PRIVACY] (providing taxonomy of sixteen aspects of privacy threats); Richards, *supra* note 17; Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

[141] Privacy scholars have recently taken interest in broadening the definition of harm caused by privacy invasions. *See, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011); Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 295–96 (2007) ("[T]he law should adapt to account for injuries to our changed conception of personhood in the twenty-first century."); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1922 (2010) (arguing that "tort law must come to a more sophisticated conception of harm").

[142] *See, e.g.*, Schwartz, *supra* note 21, at 820 ("The leading paradigm . . . conceives of privacy as a personal right to control the use of one's data.").

[143] Litman, *supra* note 138, at 1287.

that attaches to property ownership."[144] Paul Schwartz[145] and many others[146] have written in or about this vein.[147] This literature is full of calls to increase the control individuals have over their personal data.

Tort-based solutions similarly focus on control. Generally these scholars have bemoaned the inadequacy of existing tort remedies[148] and proposed additions or improvements to tort law to increase individual control.[149] Sarah Ludington has focused on the potential harm of data trading and dissemination of personal information and has proposed common law tort remedies to increase an individual's control over the use of their information.[150] Danielle Citron has focused on the harm to an individual's sense of control caused by even inadvertent information leaks from massive corporate-controlled databases and has proposed a strict liability regime to deter such leaks.[151] Neil Richards and Daniel Solove have argued for reconsidering the law of confidentiality as a means to give individuals greater

---

[144] ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 211 (1971).

[145] Schwartz has taken the nuanced view that using property to protect information privacy requires reconceptualizing what property rights in information must mean. In other words, one must limit the propertization of information but still use property as the underlying regime to protect that information. *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2058 (2004) [hereinafter Schwartz, *Personal Data*] (seeking to "develop a model for propertization of personal data that will fully safeguard information privacy"). Schwartz has argued for the propertization of personal information under certain constraints. One constraint is that data collectors should be able and required to distinguish between consumers with different privacy preferences. *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1687 (1999) [hereinafter Schwartz, *Cyberspace*]. In addition, Schwartz has called for use-transfer restrictions. In Schwartz's proposal, an individual would be free to transfer his or her own information but only if the individual could easily block further downstream transfers from the data collector to other third parties. *See* Schwartz, *Personal Data*, *supra*, at 2060.

[146] *See, e.g.*, Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 383 (2003) ("[I]n order to protect privacy, individuals must secure control over their personal information by becoming its real owners."); Adam D. Moore, *Toward Informational Privacy Rights*, 44 SAN DIEGO L. REV. 809 (2007) (arguing for increased informational privacy rights due to data aggregation and data mining).

[147] *See, e.g.*, Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1377 (2000) (arguing for legislation to create such property rights); Solove & Hoofnagle, *supra* note 109, at 358 (emphasizing personal control over information).

[148] *See, e.g.*, Julie E. Cohen, *Privacy, Ideology, and Technology: A Response to Jeffrey Rosen*, 89 GEO. L.J. 2029, 2043 (2001) ("[I]t is becoming increasingly clear that the common law invasion of privacy torts will not help to contain the destruction of informational privacy."); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000) (arguing that tort law is of limited utility in combating threats to informational privacy).

[149] *See, e.g.*, Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63 (2003) (discussing proliferation of data mining and arguing that profile collection without consent should be tortious).

[150] Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 146 (2006) (proposing an expansion of privacy tort law along fair information practices to "remed[y] the harm to an individual caused by his loss of control over his identity").

[151] Citron, *supra* note 141.

control over the use of the information they share in important relationships.[152]

Proposed legislative solutions also emphasize control rights. As Fred Cate has noted, "Virtually all privacy bills before Congress reflect this goal: 'to strengthen control by consumers' and 'to provide greater individual control.'"[153] Prescriptive informational privacy scholarship follows this pattern. Robert Sprague and Corey Ciocchetti, for example, have argued for legislation to enhance control over personal information by requiring private firms to adopt strict privacy policies.[154] Daniel Solove and Chris Hoofnagle have proposed model legislation for regulating data brokers to improve the rights of individuals[155] and for making personal information inaccessible to data miners.[156] Susan Gindin has argued for a comprehensive legislative approach to improving control.[157]

I do not disagree that control over information is important. In fact, the personal prospectus as a signaling device is only possible when individuals have control over personal information. But control is insufficient to protect privacy in an economy with low-cost signaling and the threat of unraveling. As a practical matter, unraveling simply undermines the privacy field's focus on control. Privacy advocates have not sought control just to have the *right* to keep information secret; they have sought control so that individuals have the actual *ability* to keep information to themselves. It would be a meaningless victory if the informational privacy field delivered the right to control one's information only for individuals to realize that they had no real power to do so in a signaling economy in which the stigma of staying silent requires everyone to disclose.

2. Beyond Control?.—At this point I must pause and respond briefly to the core group of privacy scholars that has attempted to liberate the concept of privacy and its protection from the constraints of control and consent. Their reaction should and likely will take the following form: "We

---

[152] *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2007).

[153] CATE, *supra* note 115, at 5 (emphasis omitted) (quoting various privacy bills).

[154] Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91, 130 (2009).

[155] *See* Solove & Hoofnagle, *supra* note 109, at 357. Their proposal covers many specific problems and solutions. Almost all, however, are grounded in improving notice and control.

[156] Hoofnagle has argued, for example, that credit-report information should be "frozen"—taken out of the public realm and made private, in the control of individuals. *See* Chris Jay Hoofnagle, *Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors*, *in* SECURING PRIVACY IN THE INTERNET AGE 207, 214–216 (Anupam Chander, Lauren Gelman & Margaret Jane Radin eds., 2008) ("Before credit could be granted, individuals would have to 'thaw' their credit by contacting a credit reporting agency and requesting release of the report.").

[157] Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1155 (1997) ("[A] comprehensive federal policy is needed which will guarantee individuals the right to control the collection and distribution of their personal information.").

agree that privacy as control is inherently flawed; we have argued as much for a decade. We have tried to move the concept of privacy well beyond control and individual consent, reconceptualizing it in various ways as a social good that deserves protection for reasons beyond individual welfare. You are tilting at windmills in fallow fields we have long abandoned."[158]

New privacy scholarship has done much to deepen our understanding of what "control" really requires, what privacy is, and why privacy deserves protection, but it has not fundamentally abandoned the idea that privacy involves control over one's information, nor the associated assumption that once an individual *has* such control, her later choice "voluntarily" to disclose such information poses no threat to privacy. Three aspects of this scholarship—and of the new approaches to privacy that it represents—undermine the argument that it has moved beyond control in ways that will prevent unraveling.

First, much new privacy scholarship has attacked existing consent processes as insufficiently protective of an individual's control over information.[159] It has pointed to the market failures in Internet information exchange that make consent to disclosure largely meaningless.[160] Websites post privacy notices that are opaque and that consumers rarely read or understand. Users click through consent forms without hesitation and often without regard for the broad rights that they are ceding to data collectors.[161] In short, "control" over one's information is relinquished too easily through implied or uninformed consent.[162]

Prescriptively, these scholars have sought to correct these market failures,[163] often by turning to Fair Information Practices (or Principles) (FIPs)

---

[158] *See, e.g.*, Cohen, *supra* note 148, at 2039 ("Modern privacy advocates . . . conceive of privacy as a species of constitutive freedom and view that freedom as both intrinsically and instrumentally valuable."); Paul M. Schwartz & William M. Treanor, *The New Privacy*, 101 MICH. L. REV. 2163, 2177 (2003) (reviewing JOHN GILLIOM, OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE AND THE LIMITS OF PRIVACY (2001)) ("These authors . . . [working on new definitions of privacy] have sought to develop a normative basis for an information privacy law based not in a right of 'individual control' over information, but in the idea of privacy as a social good.").

[159] For a description of these problems, see Max Stul Oppenheimer, *Internet Cookies: When Is Permission Consent?*, 85 NEB. L. REV. 383 (2006).

[160] *See, e.g.*, James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1181–82 (2009) (discussing statistics on how few users read or understand privacy policies). Privacy scholars have also described the weakness of consent regimes in non-Internet contexts. *See* Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 49 (1997) (describing the "shallow consent process" in health care disclosure releases).

[161] *See* Cohen, *supra* note 148, at 2041 (describing ways in which consent functions to strip users of privacy rights with little information or real control).

[162] *See* Schwartz, *supra* note 21, at 825 ("[P]rivacy-consent neglects the actual conditions of choice regarding the processing of personal information, and permits notice to become an alibi for 'take-it-or-leave-it' data processing.").

[163] *See* Schwartz, *Personal Data*, *supra* note 145, at 2082 ("The goal of market-perfecting policies should be to reform the failed privacy market to reflect more completely the varying value of personal data to individuals with different preferences about whether and how that data should be used.").

to protect information. FIPs generally require that data collection, aggregation, and storage be transparent, disclosed to individuals, secure, accurate, and limited in duration.[164] In addition, FIPs require that an individual's consent to disclosure be informed and that the individual have some ability to control downstream uses of that disclosed information in the future.[165]

Using FIPs to improve information markets by legislating data-handling and disclosure standards would undoubtedly be helpful. These steps would protect consumers against the worst excesses of data mining and dissemination.[166] But FIPs cannot, ultimately, stop unraveling. All FIPs contain provisions for voluntary, consensual disclosure of information[167] because FIPs are ultimately designed to be autonomy-enhancing.[168] FIPs are meant to remedy the market failure of uninformed, false consent but not to stop disclosure completely.[169] FIPs therefore open the door to the unraveling of privacy because, in a signaling economy, even fully informed consumers may find themselves disclosing to counter the negative assumptions attached to silence.

Second, these scholars have attempted to redefine the concept of privacy as something other than individual information control. Paul Schwartz has argued that privacy should instead be thought of as a "constitutive value" and protected because it is one of the ways in which both individuals

---

[164] There are many descriptions of FIPs. *See, e.g.*, Schwartz & Treanor, *supra* note 158, at 2181 ("Although the expression of FIPs . . . will vary in details, . . . a formulation with nine elements is possible: (1) defined limits . . . for processors of personal information (purpose specification); (2) processing systems that the concerned individual can understand (transparent processing systems); (3) notice to the individual; (4) individual choice or consent regarding the further use of her personal information; (5) security for stored data; (6) limits on data retention; (7) data quality (accurate and timely information); (8) access to one's personal data; and (9) enforcement of privacy rights and standards . . . .").

[165] *See* Avner Levin & Patricia Sánchez Abril, *Two Notions of Privacy Online*, 11 VAND. J. ENT. & TECH. L. 1001, 1009 (2009) ("The overall purpose of FIPs is to ensure that an individual will maintain control over his personal information when it is in the hands of an organization.").

[166] Schwartz's approach is to treat information as property but build inalienabilities into the definition of the property right to limit downstream transfers of the information to third parties. *See* Paul M. Schwartz, *Privacy Inalienability and the Regulation of Spyware*, 20 BERKELEY TECH. L.J. 1269, 1271 (2005) ("[T]his model would permit the transfer of personal data for an initial category of use, but only if the customer is granted an opportunity to block further transfer . . . ."). For a critique of FIPs, see Beales & Muris, *supra* note 58, at 114, which criticizes FIPs as irrelevant because consumers do not inform themselves about privacy notices and avoid decisionmaking about privacy policies.

[167] *See* LESSIG, *supra* note 51, at 228 ("These principles express important substantive values—for example, that data not be reused beyond an original consent, or that systems for gathering data be reliable—but they don't interfere with an individual's choice to release his or her data for specified purposes.").

[168] *See, e.g.*, Schwartz & Treanor, *supra* note 158, at 2164 ("The new privacy is centered around Fair Information Practices ('FIPs') and is intended to prevent threats to autonomy.").

[169] In some cases they do not achieve even this goal: notice and consent FIPs may lead only to an avalanche of privacy policies with little real control or consent by users. *See* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 341, 364 (Jane K. Winn ed., 2006) ("Notice and consent requirements often create the illusion, but not the reality, of meaningful consumer choice.").

and society are created and maintained.[170] Privacy is of value because it protects and is necessary for both the individual's self-determination and society's deliberative democracy.[171] Without it, individuals cannot equip themselves adequately to participate in a democratic collective. Julie Cohen has similarly argued that autonomy requires "insulation from outside scrutiny" so that the individual can construct a self, which is of benefit not only to the individual but to the collective as well.[172] Solove has followed a similar line.[173]

There is a valuable theoretical shift here. The argument of these privacy scholars is not just that market failures hurt the individual but also that privacy is a social good with social implications. Thus, protecting privacy rests not only on respect for individual autonomy but also on social welfare concerns about the prerequisites for a functioning polity. Under these definitions, privacy would still matter *even if* market-perfecting strategies eliminated information market failures.[174]

Yet it is important to recognize the limitations of this redefinition. None of these scholars has argued that privacy is *exclusively* a social good or constitutive value; each has recognized that individuals should retain the ability to control their information for their own ends. In other words, although the new privacy scholarship has added a definitional layer to privacy to justify its protection and regulation beyond the confines of autonomy- and control-enhancing arguments, it has not abandoned the notion that individuals do and should remain the locus of decisionmaking about their personal data. For example, Schwartz ultimately accepts that data users will incentivize data holders to disclose information. Indeed, he hopes that real consent will "create[] an entitlement in personal information and place[] pressure on the data collector to induce the individual to surrender it."[175] At a practical level, therefore, these scholars continue to assume that individuals should be able to alienate their information so long as that alienation is informed and voluntary. That assumption opens the door to unraveling.

Finally, this scholarship has continued to define "voluntary" information disclosure as not being a privacy problem or harm. Although scholars have noted the problem that commodification (or propertization) of infor-

---

[170] Schwartz, *supra* note 21, at 834.

[171] *See* Schwartz, *Cyberspace*, *supra* note 145, at 1646–47.

[172] Cohen, *supra* note 147, at 1424.

[173] *See* SOLOVE, UNDERSTANDING PRIVACY, *supra* note 140, at 92 ("Privacy protects aspects of individuality that have a high social value; it protects individuals not merely for their sake but for the sake of society.").

[174] *See* Schwartz, *Personal Data*, *supra* note 145, at 2088 ("[A] negative result for the privacy commons can occur both under privacy market failure and under a functioning market for personal data trade.").

[175] *Id.* at 2103.

mation leads to pressure to trade away that information,[176] many in the informational privacy field have nevertheless assumed that no privacy harm occurs if an individual chooses to disclose information.[177] Privacy law is grounded in classical liberal conceptions of autonomy and individualism. It assumes that invasions of privacy are damaging to autonomy and that control over information will reestablish that autonomy. What an individual does after securing control of her information is no longer a privacy issue. As Amitai Etzioni put it,

> [T]he classical liberal view of a person [is] as a free agent who knows his or her preferences and is able to act on them rationally. It reflects the ideology that to the extent that shared, inter-individual arrangements are necessary, they ought to be based on voluntary agreements or contracts between individuals—hence the notion of consent. Privacy is not violated, accordingly, if [individuals] freely consent to disclosure of information about themselves . . . .[178]

Defining privacy harm to exclude voluntary disclosure has therefore been comfortable because it squares with dominant assumptions about autonomy.

But conceding that all voluntary disclosures are beyond the bounds of privacy harm is conceding too much. To date there have been no practical consequences of this limited definition of what constitutes a privacy harm because there has been no real threat of unraveling. In a signaling economy, however, privacy law must wrestle with whether volunteering information under the pressure of the unraveling effect is truly voluntary.[179] Perhaps those with the best private information can be said to have suffered no harm in such circumstances, but what about the rest? If disclosure results solely from the pressure to defend against the inaccuracies of the digital dossier or in response to unraveling, does that not constitute a privacy problem? To the extent that privacy scholars are concerned about the broader social costs of sorting and weblining, they should see the personal prospectus and the threat of unraveling as a threat to privacy.

Articulating the exact harm of coerced disclosure is difficult. On the one hand, critics might argue that the bad driver or unhealthy insured has no "right" to keep her information private and thereby free ride on the safe and healthy in an insurance pool; that if unraveling puts pressure on those at the bottom of a pool to disclose, that will lead to more allocative efficiencies and be socially optimal. On the other hand, there are certain costs to unraveling. First, it does not feel good to be "unraveled upon." A student shared

---

[176] *See* Schwartz, *supra* note 21, at 830 ("The idea that one has a right to control her data leads inexorably to the concept of a trade in personal information.").

[177] *See, e.g.*, Calo, *supra* note 141, at 1148 ("It is not a privacy harm to use a person's information if . . . he understood and agreed to the use.").

[178] AMITAI ETZIONI, THE LIMITS OF PRIVACY 155 (1999).

[179] *See, e.g.*, Calo, *supra* note 141, at 1150–52 (acknowledging that disclosure can be coerced and that coercion exists along a spectrum such that in some circumstances one's decision to volunteer information can be tantamount to coercion).

with me the anecdote that she was very frustrated to discover that a female peer was telling all potential employers during interviews that she did not wish to have children in the next five years. This disclosure put pressure on all female candidates in the pool to say something similar for fear that silence would be interpreted adversely. She felt invaded by her peer's disclosure, which seemed strategic and which forced her to share (or distort) information she otherwise would not.

The idea that putatively voluntary disclosure can sometimes constitute privacy harm is relatively radical, however. As Cohen has argued, "the unfettered use of 'true' information to predict risk and minimize uncertainty is a hallmark of the liberal state and its constituent economic and political markets."[180] The need for rationalizing information to price risk, sort consumers, and the like both drives invasive maneuvers to access information like the digital dossier and leads to attempts to induce its disclosure like the personal prospectus. Redefining such disclosure as a privacy harm—at least in some circumstances—counters this inherent tendency and the assumption behind it that more information is almost always of social benefit.

III. UNRAVELING'S LIMITS AND LIMITING UNRAVELING

Let us summarize the argument to this point. Verifiable signals theoretically lead to unraveling as all individuals in a pool find it in their self-interest to disclose at first for measurable economic gain and eventually to avoid the stigma attached to silence. The informational privacy field has largely ignored the threat of signaling. This has had little consequence to date because sorting dominated the economy; signaling remained nascent because low-cost verification was impossible. Signaling is becoming low cost, however, thanks to digital monitoring of directly observable data and digital access to directly verifiable data. Therefore, serious attention to the problem of privacy's unraveling is required.

This Part takes up that challenge. I do not advocate for a draft statute or call for the creation of a new regulatory agency. The unraveling effect permits neither simple nor comprehensive solutions. Instead, I explore three foundational issues for the informational privacy field as it considers confronting unraveling. First, what are the known limits of the unraveling effect, and will those limits aid in preventing privacy's unraveling in a signaling economy? Second, in what ways can the law curtail or prevent unraveling, and will they protect privacy? Third, will privacy advocates be able to muster sufficient support for such legal constraints on unraveling?

Throughout, I take the threat of unraveling seriously without assuming that it necessarily results in the end of privacy. There are ways to dampen its effects, and privacy scholarship must focus more intently on those dampening mechanisms. Nonetheless, privacy advocates should be sobered by

---

[180] Cohen, *supra* note 148, at 2030.

the rise of a signaling economy: the personal prospectus complicates informational privacy both in theory and in practice.

A. Limits on Unraveling

One possible counterargument at this point could focus on the known limits of the unraveling effect. Not all information markets unravel. Instead, unraveling is limited by transaction costs, ignorance of desired information, inability to accurately make negative inferences, and social norms. This section explores what we know about the limits of the unraveling effect.[181] It may provide some reassurance for privacy advocates who are hopeful that unraveling will not occur. Ultimately, however, I conclude that most of the known limits on unraveling will do little to preserve privacy in the evolving signaling economy.

1. Transaction Costs.—Research shows that unraveling may be partial or incomplete when it is costly to disclose information,[182] costly to acquire it,[183] or difficult for the informed party to credibly communicate the information to her uninformed counterpart.[184] There are no surprises here—the ability to signal at low cost is the precondition for the unraveling effect. If signals are cost-prohibitive to send or receive or if no verifiable signals exist,[185] unraveling cannot occur.

A recent study of the online auto auction site eBay Motors demonstrated, for example, that the cost of disclosure affects how much a seller will post in an online auction and therefore also affects the functioning of the market.[186] Some information relevant to such an auction is easily disclosed ex ante and easily verified ex post. Pictures of the car's exterior condition, for example, fall into this category. This information unravels towards full disclosure—sellers disclose such pictures because it is low cost to do so, the

---

[181] This section reviews some of the main constraints on unraveling. For an overview including other constraints, see David Dranove & Ginger Zhe Jin, *Quality Disclosure and Certification: Theory and Practice* (Nat'l Bureau of Econ. Research, Working Paper No. 15644, 2010), *available at* http://ssrn.com/abstract=1537763.

[182] *See* Boyan Jovanovic, *Truthful Disclosure of Information*, 13 BELL J. ECON. 36 (1982) (explaining that transaction costs inhibit the effect).

[183] *See* Farrell, *supra* note 133.

[184] *See, e.g.*, Steven Shavell, *A Note on the Incentive to Reveal Information*, 14 GENEVA PAPERS ON RISK & INS. 66 (1989) (exploring distinction between unraveling with verifiable versus unverifiable information).

[185] It is worth noting that in some instances the lack of verifiability does not necessarily prevent unraveling. In some markets, early disclosures begin with those seeking to signal enthusiasm or willingness to cooperate even if they cannot directly signal their overall quality. *See* Sam-Ho Lee, *Jumping the Curse: Early Contracting with Private Information in University Admissions*, 50 INT'L ECON. REV. 1, 3–4 (2009) (analyzing early college admissions data and arguing that although admissions officers cannot directly observe student quality, they accept greater numbers of early applicants to identify enthusiasts).

[186] *See* Gregory Lewis, *Asymmetric Information, Adverse Selection and Online Disclosure: The Case of eBay Motors*, 101 AM. ECON. REV. 1535 (2011).

photographic representation of the car is verifiable when the buyer takes possession, and the failure to post such photos is therefore taken as a signal that there is something to hide.[187] The author of the study noted that "[w]here bandwidth and technology are available to tightly define the contract between buyer and seller through rich media such as photos and videos, adverse selection problems are mitigated."[188] As disclosure costs increase, however, disclosure does not occur.

This suggests that the unraveling of privacy is unlikely to be quick or uniform across information contexts. The costs of signaling are dropping in some areas as technologies make verifiable disclosure much less expensive. Health monitoring is one example; monitoring of employees and equipment is another. In other areas, costs may come down more slowly. The second component of the personal prospectus—digital access to directly verifiable data—may take longer to evolve across the economy, and it is difficult to predict how the costs of the infrastructure needed to produce such real-time verified access to information will be distributed. If an individual ties her personal prospectus to her employer's database, the employer must expend resources to answer queries about her employment record. Similarly, if a personal prospectus is tied to a government database (e.g., criminal history or tax records), the state will be asked to subsidize the verified sharing of that information. Who will pay for such data structures and processes? As these questions are worked out across the economy, some information may not be available to the personal prospectus. In such domains in which disclosure costs remain high, unraveling may not occur or may be delayed.

The argument of Parts I and II suggests, however, that as a general proposition the costs of signaling are decreasing and therefore the threat of unraveling is increasing. These transaction cost constraints therefore offer limited reassurance if one fears the unraveling of privacy.

2. Unverifiability of Ignorance.—Some types of information are inherently difficult to verify not because of the transaction costs involved, which a signaling economy may overcome, but rather because the information type makes verifiability impossible. Masahiro Okuno-Fujiwara, Andrew Postlewaite, and Kotaro Suzumura revealed this problem.[189] They explained it in the context of the crate of oranges example discussed in the Introduction. Imagine that the seller is ignorant of the number of oranges in the crate.[190] Assume that there is no way for the seller to certify his ignorance to the buyer. He cannot prove that he does not know the number of

---

[187] *Id.*

[188] *Id.* at 1546.

[189] *See* Masahiro Okuno-Fujiwara, Andrew Postlewaite & Kotaro Suzumura, *Strategic Information Revelation*, 57 REV. ECON. STUD. 25, 27 (1990) ("[O]ur paper emphasizes how restrictive are the conditions which guarantee the revelation of information in equilibrium.").

[190] *See id.* at 45 (explaining that one type of unverifiable information is "a case in which [a] person's type might correspond to his not knowing something").

oranges. Nor could a court or other outside reviewer easily prove that negative. As a result, the buyer cannot know whether to draw a negative inference from the seller's silence. If the seller remains quiet, is it because there are few oranges in the crate or because the seller is merely ignorant of the number of oranges? This may lead to those with "good" information disclosing but not to a complete unraveling of all sellers' information.[191]

A similar but more general constraint occurs merely if the uninformed party does not know the kind of information held by the informed party. A buyer must know that the seller has information about product quality before product quality can unravel towards full disclosure.[192] For example, restaurants did not typically disclose health reports until required by law to do so because consumers did not seem to realize that the restaurants had such reports on hand. Similarly, if a buyer does not know that a used car salesman has information about recent repairs to a car, the buyer cannot draw negative inferences from the salesman's silence.[193]

These ignorance constraints do not seem likely to dampen the potential unraveling of privacy by the personal prospectus although they may have some effect. In most relevant instances of individual-to-individual interaction or consumer-to-firm exchange, there is common knowledge[194] that the individual has information of a certain type. An insurance company knows that you know how much junk food you eat, and you know they know that you know. A car rental company knows that you know how fast you are driving and where you are going. An employer knows that you know whether you were at work during a given time period or whether your educational qualifications are represented properly on your resume. There is no ignorance constraint in such contexts.

3. Inability to Accurately Infer a Negative.—Another possible constraint is whether the uninformed can accurately draw negative inferences from nondisclosure. Michael Fishman and Kathleen Hagerty's work has

---

[191] *See* BAIRD, GERTNER & PICKER, *supra* note 14, at 95 ("Unraveling may not occur (or will not be complete) if there is a chance that a player has never acquired the relevant information. In such a case, one will not be able to tell whether players are silent because they do not have the relevant information or because they have the information but do not wish to reveal it.").

[192] *See* Paul Milgrom & John Roberts, *Relying on the Information of Interested Parties*, 17 RAND J. ECON. 18, 19–20 (1986) ("If the interested party has known monotone preferences over the decision-maker's choice set (e.g., a seller wants to sell as much as possible, an electric utility company prefers less restrictive emissions standards) and has information that bears on the decisionmaker's preferences, and if the decisionmaker knows what information to seek, then (i) the decisionmaker's unique equilibrium strategy is to *assume the worst* . . . and (ii) the equilibrium decision is the *full-information decision* . . . .").

[193] *See id.* at 20 (using this example and noting that "the decisionmaker must know the factors about which the interested party has information to detect situations in which information is being withheld").

[194] BAIRD, GERTNER & PICKER, *supra* note 14, at 304 ("Something is common knowledge if it is known to each player, and, in addition, each player knows that the other player has this knowledge; knows that the other person knows the player knows it; and so forth.").

shown, for example, that for unraveling to occur the uninformed receiver of signaled information must be able to understand the disclosed information and actually draw negative inferences from nondisclosure.[195] If consumers do not draw negative inferences from silence, sellers have no incentive to disclose product information.[196] Some have suggested that this explains the failure of most hospitals to disclose evaluations of their quality—patients seem to naïvely believe that their doctors are above average even without disclosure, and therefore unraveling does not get started.[197] More generally, unsophisticated actors may not think strategically and may be naïvely credulous. If informed sellers believe this, for example, they will fail to disclose and will treat every buyer as if he is unsophisticated.[198] Only when the uninformed parties in a market consist of a sufficient number of sophisticated players will unraveling occur and force disclosure by informed parties.

In addition, some information types make it hard to draw negative inferences accurately, and therefore informed parties may not fully disclose. In one landmark study, Alan Mathios examined why some salad dressing manufacturers failed to provide nutritional information before being required to do so by law.[199] In theory, no mandatory disclosure law should have been necessary. The unraveling effect primarily requires that disclosures be truthful, that is, that a seller cannot lie about product quality. The law need not require full disclosure to produce it.[200] Instead, in a competitive market truthfulness can lead to full disclosure as high-value or high-quality individuals signal their quality early, beginning the unraveling.

Mathios compared salad dressing labeling before and after the passage of the Nutritional Labeling and Education Act (NLEA).[201] He found that

---

[195] *See* Michael J. Fishman & Kathleen M. Hagerty, *Mandatory Versus Voluntary Disclosure in Markets with Informed and Uninformed Customers*, 19 J.L. ECON. & ORG. 45 (2003).

[196] *See* Joel Huber & John McCann, *The Impact of Inferential Beliefs on Product Evaluations*, 19 J. MARKETING RES. 324 (1982) (studying consumer skepticism in the absence of disclosure about product characteristics); Richard D. Johnson & Irwin P. Levin, *More Than Meets the Eye: The Effect of Missing Information on Purchase Evaluations*, 12 J. CONSUMER RES. 169 (1985).

[197] *See* DAVID DRANOVE, CODE RED 91 (2008) (calling this "Lake Woebegone Syndrome").

[198] *See* Milgrom & Roberts, *supra* note 192, at 20 ("[A] rational salesman will treat every buyer as if he were naively credulous.").

[199] *See* Alan D. Mathios, *The Impact of Mandatory Disclosure Laws on Product Choices: An Analysis of the Salad Dressing Market*, 43 J.L. & ECON. 651 (2000); *see also* Rebecca S. Fribush, Note, *Putting Calorie and Fat Counts on the Table: Should Mandatory Nutritional Disclosure Laws Apply to Restaurant Foods?*, 73 GEO. WASH. L. REV. 377 (2005) (extending theory to restaurant disclosures).

[200] Mandatory disclosure versus voluntary or unraveling disclosure is a hugely debated topic. Grossman began the discussion. *See* Grossman, *supra* note 131. Others have continued the debate. *See* Joseph A. Franco, *Why Antifraud Prohibitions Are Not Enough: The Significance of Opportunism, Candor and Signaling in the Economic Case for Mandatory Securities Disclosure*, 2002 COLUM. BUS. L. REV. 223.

[201] Nutritional Labeling and Education Act of 1990, Pub. L. No. 101-535, 104 Stat. 2353 (codified as amended at 21 U.S.C. § 301 (2006)).

before the NLEA, when labeling was voluntary, low-fat dressings consistently used nutrition labels but those with more fat did not. He attributed this finding to the fact that a consumer may have difficulty assigning a negative weight to the undisclosed fat content, because it is theoretically unbounded. If all dressings with fewer than ten grams of fat have labels and all above ten grams do not, any given unlabelled dressing could have from eleven grams to infinity. "For a nutrient with negative health consequences, consumers must infer how inferior is the product from the worst of the disclosed products, and economic theory cannot accurately bound this amount."[202] In other words, very high-fat dressings can hide in a pool with moderately high-fat dressings because at some point consumers fail to distinguish between them and the costs of differentiating may outweigh the benefits.

Positive characteristics, in contrast, are all likely to be disclosed because there is a natural lower bound of zero. Thus, if a product contains a nutrient with positive health consequences, all manufacturers of such products will likely disclose the amount of said nutrient. Failure to disclose will lead to the assumption that none of the nutrient is present.

These results suggest that privacy may not completely unravel because of the personal prospectus. Even if those with the very best traits disclose fully, not everyone may be forced to follow. At some point market participants may stop drawing the negative inferences needed to drive unraveling, and therefore the very worst may be able to pool together with the remaining middle of the set of persons, products, or firms in question. Economic theory cannot predict when exactly this will occur: it is an empirical question dependent on the specifics of the given market. But this suggests that in some instances the equilibrium may allow some market participants with less than ideal information to keep that information private.[203]

Yet this is little consolation. In many of the examples discussed here, the uninformed players are homogeneous in their sophistication, and they are seeking information that is bounded in some fashion. We can assume that insurance carriers, for example, are sophisticated and will draw negative inferences from insureds' silence. Further, they seek positive information about health characteristics or behaviors that is not subject to Mathios's boundedness problem: for example, whether a given insured smoker keeps her blood glucose below a certain level. Note the potential asymmetry, however, this suggests between consumers and firms—although firms may typically unravel consumers' privacy, consumers may not necessarily force disclosure by firms if one assumes that consumers are not homogeneously sophisticated in their game theoretic inferences.

---

[202] Mathios, *supra* note 199, at 674.

[203] Even so, the participants with less than ideal information will still be lumped together with the others at the bottom of the particular quality spectrum.

4. Norms.—Finally, privacy norms sometimes develop that constrain unraveling. Judge Posner gives the example of the market for physical attractiveness. Beautiful people have an obvious incentive to reveal their attractiveness by wearing little or no clothing whenever possible. In an unraveling of sorts, those who remain covered should be assumed to be less desirable.[204] In equilibrium, everyone should become a nudist. This is not, of course, the case. The norm against nudity prevents disclosure. This norm could have developed for many reasons, including the potential inefficiencies of widespread nudity. The point, however, is simply that in some cases norms prevent unraveling.

A recent study of SAT score disclosure by college applicants seems to support the notion that norms can constrain disclosure. Over seven hundred colleges and universities now make disclosure of SAT scores voluntary. One would expect that this would do little to change the market—those with high scores should reveal, leading to an unraveling equilibrium and full disclosure by all applicants. Analysis of actual data by roughly 3000 applicants, however, reveals that although those with the highest scores do disclose, not all in the middle range do so. Instead, both African-Americans and female applicants were more likely to withhold their scores even when the scores were of reasonable, if not the very highest, quality.[205] The authors hypothesize that informal norms may have developed among African-Americans and women: in particular, that the SAT test is biased, discriminatory, and unfair. As a result, individual members of these groups may resist disclosure even when their SAT scores are above average.[206]

To the extent that informal norms develop against disclosure, privacy may not unravel completely. Sometimes individuals will incur economic costs to defend a norm that produces other personal or social benefits, as the SAT study seems to demonstrate. In most cases, however, privacy norms seem better at constraining the sharing of information with low economic value but high prurient interest—for example, gossip or nudity norms.[207] Norms are less likely to evolve to protect information that is economically valuable, particularly when some set of actors will *want* the ability to disclose such information. As a result, norms do not seem likely to prevent the unraveling effects of a signaling economy.

---

[204] *See* POSNER, *supra* note †, at 107 (discussing this example).

[205] *See* Gabrielle Chapman, Michael Conlin & Stacy Dickert-Conlin, The Economics of Voluntary Disclosure in SAT Scores (Aug. 17, 2004) (unpublished manuscript), *available at* https://www.msu.edu/~dickertc/301f06/SAT.pdf.

[206] *See id.* at 17.

[207] *See* Richard H. McAdams, *Group Norms, Gossip, and Blackmail*, 144 U. PA. L. REV. 2237, 2279–82 (1996) (describing norms against disclosing or asking for information that has little social function beyond being titillating gossip).

B. Limiting Unraveling: Comparing Regulatory Strategies for Preserving Privacy

Privacy advocates can take some reassurance from these limits: unraveling may be slow and lumpy across the economy as disclosure costs drop differently in different contexts; some contexts may experience only partial unraveling; norms may sometimes counter unraveling. But this review of the empirical limits of the unraveling effect generally reinforces Part II's argument that privacy is increasingly threatened by signaling. Privacy advocates must therefore turn to the legal constraints that might prevent unraveling.

1. Don't Ask, Don't Tell?[208].—Inquiry limits and disclosure limits ("don't ask" rules and "don't tell" rules) are often used to protect personally or socially sensitive information.[209] Inquiry limits forbid an uninformed party from seeking information from an informed counterpart.[210] For example, the Americans with Disabilities Act (ADA) forbids an employer to ask a potential employee about disabilities,[211] and the regulations implementing Title IX of the Education Amendments of 1972 similarly forbid inquiry about marital status by employers. Likewise, various states bar inquiries about religious or political affiliations during the hiring process.[212]

Inquiry limits rarely seem to inhibit unraveling, however.[213] Economists have long recognized that the unraveling effect will typically render an inquiry limit ineffective. Robert Frank considers the problem of employment discrimination regulations:

---

[208] A related option is "don't know" rules. In some instances, the best means to prevent unraveling is to never learn or store the information to begin with. Some have suggested using technology to limit an individual's *ability* to disclose information, for example. James D. Miller and Lixin Gao propose that presidents and public officials keep encrypted diaries to which even they do not have access until their deaths, thereby preventing the unraveling effect from forcing disclosure of personal notes. This would promote historical record-keeping but would curtail the unraveling problem that would be presented if the public knew that a president had a personal diary with information relevant to a scandal or investigation but refused to (and could not be forced to) turn it over. Like the crate of oranges, the president's silence would be interpreted as an indication that the diary contained negative information. Thus, only if the president *could not* release the encrypted diary would it be rational for a president to keep a diary. In other words, by encrypting the information even as against its author, one would eliminate the negative inference that the public would draw in the event that it sought access to the diary but was denied. *See* James D. Miller & Lixin Gao, *Creating a Subpoena-Proof Diary: A Technological Solution to a Legal Problem*, 3 J. INFO. L. & TECH. (2001), http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/miller.

[209] The most infamous example of a "don't ask, don't tell" policy was the military's stance towards homosexual and bisexual service members. *See* 10 U.S.C. § 654 (2006), *repealed by* Don't Ask, Don't Tell Repeal Act of 2010, Pub. L. No. 111-321, 124 Stat. 3515.

[210] Gertner, *supra* note 14, at 605 ("Inquiry limits are legal rules that try to restrict the ability of an uninformed party to ask for disclosure from informed parties.").

[211] *See* 42 U.S.C. § 12112(c)(4)(A) (2006).

[212] *See* BAIRD, GERTNER & PICKER, *supra* note 14, at 92 (discussing these examples).

[213] *See id.* ("Inquiry limits . . . may be ineffective unless there is some mechanism that prevents voluntary disclosure of the information.").

> Consider . . . legislation that prohibits employers from asking about marital status and plans for having children. . . . [I]t is not sufficient merely to prohibit employers from asking about demographic categories. For if a woman realizes that her own particular situation places her in the most favored hiring category, she has every incentive to *volunteer* the relevant information. This sets up the familiar unraveling process whereby all but the least favorable information will eventually be volunteered freely by job candidates. The candidate who fails to volunteer information, however unfavorable, is simply assumed to be in the least favorable category. If the legislation were to achieve its desired intent, it would somehow have to prohibit job candidates from volunteering the information at issue.[214]

This sort of unraveling is exactly what one finds in job markets. Empirical examination of resumes shows that job candidates very often reveal information to potential employers that they need not, probably to signal traits that they perceive will assist them in their quest for employment.[215]

Given this problem, there are contexts in which we deploy disclosure limits. We forbid banks and bank examiners from discussing bank examinations publicly, for example, for fear that unraveling will weaken the banking system when it is already under stress.[216] The unraveling problem is obvious: banks with good reports will disclose their relative health; the public will run to those banks; this will damage less healthy banks that might have been able to survive with assistance but cannot survive the flight of their customers. Unraveling would impose serious social costs, and we have therefore limited disclosure of this information.

It is difficult to imagine strong disclosure limits as a comprehensive solution to the unraveling of privacy, however. The banking context is a somewhat unique circumstance. Banks are highly regulated entities already subject to a host of disclosure and information constraint rules. By contrast, individuals, who are protected by the First Amendment, are unused to such micromanaging of their speech. It would be bizarre and unconstitutional, for example, to forbid self-disclosure on one's resume. In addition, the social costs at stake are high in the banking context. It is not clear that the social justifications for limiting disclosure are as salient or pressing in most of the informational privacy contexts discussed to this point. In fact, in many cases signaling permits allocative efficiencies. It is hard to imagine how one would overcome the constitutional and social objections that would be

---

[214] FRANK, *supra* note 16, at 107–08.

[215] *See, e.g.*, Lynne Bennington & Ruth Wein, *Aiding and Abetting Employer Discrimination: The Job Applicant's Role*, 14 EMP. RESPS. & RTS. J. 3, 9–12 (2002) (empirically reviewing applicants' resumes and finding the inclusion of unnecessary information that could aid an employer in discriminating against the employee).

[216] *See* BAIRD, GERTNER & PICKER, *supra* note 14, at 94–95 ("Because of the unraveling principle, the law works only if limits are placed on a bank's ability to talk about a report, regardless of whether it is favorable.").

raised were one to broadly prohibit individuals from sharing their personal information.

In addition, even were one to impose broad disclosure limits to protect information, there are sometimes other signals that interested actors can use to communicate the same information without violating the disclosure limit. A recent study of need-blind college admissions policies demonstrates this problem.[217] Various elite colleges and universities publicly proclaim that they admit on a need-blind basis. They do not ask about financial need and do not accept applications that disclose it. Nevertheless, the schools have obvious economic interest in not admitting too many financially needy applicants, for fear of overwhelming the schools' scholarship funds. To end-run around the don't ask, don't tell regime, schools may simply admit a disproportionate number of early admissions applicants. Admissions officers know that those needing financial aid are less likely to apply for early decision because the binding early decision process prevents them from comparing financial aid packages across different universities. Schools can therefore limit their exposure to need-blind admissions policies while maintaining their public commitment to being need-blind by disproportionately admitting early applicants.

This secondary signaling would likely also occur were we to adopt widespread limits on inquiry and disclosure to prevent unraveling in health care, car insurance, employment decisions, and elsewhere. When both sides of an information exchange have an incentive to share a verifiable piece of information and can do so at low cost, it is difficult to prevent them from finding some means to transmit such a signal.

2. Don't Use?.—This leaves privacy advocates with rules that restrict the use of information, regardless of how it has been shared. "Don't use" rules prohibit a decisionmaker from considering certain information even if that information is relevant to the decision. Fifth Amendment jurisprudence, for example, requires a judge to order a jury not to draw negative inferences from a defendant's failure to testify.[218] The Fair Credit Reporting Act[219] bars creditors from inquiring about or denying credit on the basis of bankruptcies more than ten years old.[220] Some states have limited car rental companies from using data from GPS monitors to penalize consumers.[221] And our health care statutes limit an insurer's use of information about an

---

[217] *See* Matthew Kim, *Early Decision and Financial Aid Competition Among Need-Blind Colleges and Universities*, 94 J. PUB. ECON. 410, 414 (2010) (explaining this result).

[218] *See* Carter v. Kentucky, 450 U.S. 288 (1981). For discussion of this example in the context of unraveling, see Gertner, *supra* note 14, at 605.

[219] 15 U.S.C. § 1681 (2006).

[220] *Id.* § 1681c(a)(1).

[221] *See supra* notes 85–90 and accompanying text.

insured's medical condition when the insurer is setting coverage or premiums.[222]

More recently, Congress has enacted a powerful "don't use" rule to prevent information unraveling in the context of genetic discrimination.[223] Individuals in possession of good genetic test results have an incentive to reveal that information to insurers; insurers will then lump together those who make no such disclosures as being of greater risk.[224] Although some scholars have advocated for the efficiencies of total disclosure,[225] privacy and health advocates have long sought to prevent the use of genetic information by an insurer as a basis for adjusting insurance premiums or making coverage decisions.[226] The 2008 Genetic Information Nondiscrimination Act (GINA) is one example: it bars the use of genetic information by insurers to prevent unraveling.[227]

Don't use rules are more likely to constrain unraveling than don't ask or don't tell rules. They are the best means for privacy advocates that wish to prevent or constrain unraveling. At the same time, don't use rules are often difficult to enact. Congress considered GINA for over a decade, and even after its enactment many doubt whether the enforcing regulations will really be able to prevent the use of genetic information completely. Such rules are inherently paternalistic. They rest on a social judgment that even if transacting parties both wish to reveal and use a particular piece of information, its use should be forbidden because of some social harm, such as discriminating against those with genetic disorders, that is greater than the social benefits, such as the allocative and contractual efficiency created by allowing freedom of contract. It is no surprise that these examples of strong don't use rules arise in the context of racial, gender, and genetic discrimination—areas in which there are strong legislative sentiments, galvanized political will, and the social consensus that discrimination based on these immutable characteristics should be prevented. These rules were not the result of privacy debates so much as the result of debates over the social costs of discrimination generally.

---

[222] *See supra* notes 27–31 and accompanying text.

[223] *See* Sagit Ziskind, *The Genetic Information Nondiscrimination Act: A New Look at an Old Problem*, 35 RUTGERS COMPUTER & TECH. L.J. 163, 196–97 (2009) (exploring how those with good genetic results will likely disclose such results to insurers, leading insurers to ultimately discriminate against those who disclose nothing).

[224] *Id.* at 198.

[225] Kathleen Taradash, Comment, *Preventing a Market for "Lemons": A Voluntary Disclosure Model as an Alternative to the Prohibition of Genetic Discrimination and the Distortion of Allocative Efficiency*, 34 CONN. L. REV. 1353, 1379 (2002) ("In the privacy quid-pro-quo, employers who need access and use of individual genetic information will offer sufficient incentives to encourage the other party to disclose.").

[226] *See* Ziskind, *supra* note 223, at 200 ("The best practical solution is . . . comprehensive protection against health insurers' use of genetic information . . . .").

[227] *See* Pub. L. No. 110-233, §§ 101–105, 122 Stat. 881, 883–904.

C. The Public Choice Problems of Limiting Unraveling

This brings us to our final and perhaps most fundamental discussion: does the informational privacy field have any practical chance of countering unraveling effects in a signaling economy? The informational privacy field has lamented the difficulties of enacting legislative privacy reforms.[228] There is no comprehensive federal privacy statute, and state statutes are erratic and incomplete.[229] Despite many legislative proposals by scholars and privacy advocates, they have not garnered legislative support. These proposals have focused on increasing individual control over information to protect privacy against the threat of the digital dossier. [230] These control proposals have largely failed.

The implications of this history are ambiguous. On the one hand, one could certainly argue that enacting constraints on signaling and unraveling will be *more* difficult than enacting control rights. To agree to control rights a legislator does not need to face dead-on the paternalism problems inherent in don't use rules. Instead, control proposals can hold on to the chimera that control will give individuals autonomy and the freedom to decide what to do with their private information. This is a relatively comfortable stance, grounded in liberal assumptions about individuality, autonomy, and alienability. But a signaling economy and the threat of information unraveling undermines this comfortable position, instead requiring difficult judgments about restricting the use of information regardless of individuals' desires. One might therefore draw the conclusion that the privacy field's inability to even enact comprehensive control reforms suggests that addressing the signaling economy will be next to impossible.

On the other hand, perhaps employing "don't use" rules to combat problematic signaling will be easier than control prescriptions in some respects. The privacy field has been ineffective in part because its narrative about the harms of sorting and the digital dossier is too abstract to whip up any legislative or public response. The threat has seemed intangible—the prospect of data aggregators targeting consumers for certain products or more accurately assessing credit risks may not be concrete enough to make legislators take notice. More bluntly, such descriptions of the digital dossier's harms may simply not be enough to counter the powerful lobbying voices of the firms and industries that benefit from increased sorting accuracy.

Intriguingly, however, legislative response to signaling and unraveling problems has sometimes been relatively quick and decisive. California, New York, and Connecticut each jumped on the use of GPS-enabled tracking devices by car rental companies after the first consumer complaints be-

---

[228] *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009).

[229] *See id.* at 917–22.

[230] *See supra* Part II.B.

gan.[231] Various states have forbidden employers from requiring employees to accept subcutaneous RFID tags even before employers had a chance to experiment with such technology. GINA is now in place, even before widespread access to genetic information is available to the average consumer. It is easy to imagine legislatures reacting strongly to perceived abuses or the threat of abuses of home or personal health monitors, smart grid technology, and other tracking and monitoring devices. These examples suggest that in some contexts the threats created by the signaling economy are more tangible and salient than those of the digital dossier, and thus perhaps the privacy field may have *more* success in this new arena than it has had protecting control over information generally.

The challenge for any regulatory strategy will be overcoming the self-interest of those that wish to signal their positive characteristics. The most dramatic difference between this future fight against unraveling and the battle that privacy advocates have fought to date is that to this point the privacy field has been able to frame the digital dossier as firms-versus-consumers. In the world of the digital dossier, unnamed data aggregators surreptitiously appropriate and use your data to sort you, without your knowledge and to potentially harmful effect. The legislative contest has been to galvanize the polity to see this phenomenon as a threat. In the signaling economy, however, the frame must shift. No longer will the debate merely be firms-versus-consumers; now the contest will turn into consumer-versus-consumer as groups that desire to signal for personal gain will oppose those seeking to block the use of information for fear of unraveling.

The ability to disclose—even at the risk of unraveling privacy—brings with it the ability to seek economic advantage. There are distributive stakes here. As George Stigler has noted,

> There is a redistribution of income within a class when classes are made less homogenous. When it becomes more difficult to measure differences among individuals, their treatment becomes more uniform. Lower and higher risk credit are treated as average risk credit, and similarly with the traits of workers, students, and others. It [becomes] a little easier to default on consumer credit, to embezzle funds, and to shirk duties. A redistribution of income takes place within the enlarged class.[232]

Fighting privacy's unraveling will provoke resistance from those who wish to be able to distinguish themselves from the average. Those with the "best" traits or characteristics will sense the redistributive nature of don't ask, don't tell, and don't use constraints. There will thus be natural constituencies to advocate for disclosure, and those constituencies are likely to contain the powerful, educated, and affluent. Not only will firms and indus-

---

[231] *See supra* Part I.C.

[232] George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 630 (1980).

tries seeking information advocate for disclosure, but those consumers that can attain advantages through disclosure will as well.

In addition, unraveling will be incremental, not sudden. Privacy advocates will undoubtedly find it difficult to articulate clearly why they object to any one small increase in disclosure, which in isolation may well look welfare maximizing. Monitoring blood alcohol limits *is* a good idea to combat drunk driving, car insurance discounts *do* provide benefits, and iris-scanning or other identity-revelation *can* prevent and control crime. Together, however, these individual examples of unraveling information combine to create a world in which greater and greater amounts of—perhaps all—information becomes known or shared. This is the full disclosure future that privacy advocates have questioned, brought about by signaling instead of (or together with) sorting and data mining.

In such a world, opponents of disclosure and signaling will fall into one of two categories: those with negative traits or information that they wish to hide and privacy advocates who see some social threat or harm from disclosure that overwhelms any individual benefit. The first group will be easy to ignore, at least when the information they seek to protect does not concern an immutable characteristic like race, gender, or genetics but instead a behavioral one such as criminal history or educational background. The second group is the informational privacy field itself. It will face the difficult task of articulating the social harm of unraveling to spur legislative action.

CONCLUSION

The economy is changing, and privacy law must change as well. I do not have easy prescriptions to offer—my purpose has been to outline a significant new challenge to privacy. To remain relevant, the field of informational privacy law must address the unraveling problem that has to this point been merely a theoretical curiosity. The dominant syllogism in privacy theory must yield to new conceptions of privacy interests and to new arguments about why unchecked signaling should be considered a harm. If privacy advocates fear a future of full disclosure, they must articulate why. In a signaling economy, they will face even *more* organized opposition to restricting information disclosure than they have faced to date. Their task, in short, is becoming harder, not easier, as the personal prospectus grows, the signaling economy evolves, and privacy continues unraveling.