

**UNRAVELING PRIVACY:  
THE PERSONAL PROSPECTUS &  
THE THREAT OF A FULL DISCLOSURE FUTURE**

*Forthcoming* Northwestern University Law Review (2011).

By 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.

-- Richard Posner<sup>1</sup>

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, doesn't drive much after midnight, and avoids frequently slamming on the brakes, at the end of the year he receives up to twenty-five percent 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."<sup>2</sup> To date, Progressive Insurance's MyRate program<sup>3</sup> is available in twenty states and has enrolled roughly ten thousand customers. Other insurance companies are following suit.<sup>4</sup> Some carriers are going further, offering discounts for the use of more sophisticated devices that record geographical location, minute-by-minute speeding violations, and whether seat belts are in use.<sup>5</sup> Rental car

---

\* Associate Professor of Law, University of Colorado School of Law. I thank my colleagues at the University of Colorado Law School for their interest in and feedback on this project, particularly Paul Ohm, Vic Fleischer and Phil Weiser. I thank Mark Gibson and Matt Burns for their excellent research assistance.

<sup>1</sup> Richard Posner, *Privacy*, in 3 THE NEW PALGRAVE DICTIONARY OF ECON. & THE LAW 103 (1998) [hereinafter Posner, *Privacy*].

<sup>2</sup> Bengt Halvorson, *Car Insurance Savings Come With 'Big Brother,'* <http://www.cnn.com/2009/LIVING/wayoflife/05/22/aa.pay.as.drive.insurance> (last visited July 9, 2010).

<sup>3</sup> See <http://www.progressive.com/myrate> (last visited July 9, 2010). The program was recently renamed Snapshot and updated slightly. See *id.* (last visited August 3, 2010).

<sup>4</sup> 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) (discussing various plans). GMAC Insurance, for example, uses OnStar data to track total miles driven. See <http://www.gmac123.com/auto-insurance/smart-discounts/low-mileage-discount.asp> (last visited July 1, 2010).

<sup>5</sup> See [www.anpac.com/drivesmart](http://www.anpac.com/drivesmart) (last visited July 12, 2010). 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, whether seat belts are in use, 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*

companies have also experimented with using such monitors to incentivize safe driving.

Similarly, every day the Mayo Clinic in Rochester, Minnesota uses remote monitoring devices to check up on the health of residents at the nearby Charter House senior living center. The devices transmit data about irregular heart rhythm, breathing rate, and the wearer's position and motion. "The goal," says Dr. Charles Bruce, the lead investigator on the project, "is to have full remote monitoring of people, not patients, just like you measure the pressure of your tires today."<sup>6</sup> 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,<sup>7</sup> and GlySens is working on an implantable subcutaneous blood sugar sensor for diabetics that uses the cellular network to constantly send real time results to one's doctor.<sup>8</sup> 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, such "pervasive lifestyle incentive management" is already being discussed by those in the healthcare field.<sup>9</sup>

Finally, every day tenants, job applicants, and students voluntarily disclose verified personal information to their prospective landlords, employers, and safety-conscious universities using online services such as MyBackgroundCheck.com.<sup>10</sup> 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 "resume enhancement."<sup>11</sup>

---

*Car*, NEW YORK TIMES (July 7, 2010). Event recorders may become mandatory in new vehicles. See Motor Vehicle Safety Act of 2010, S. 3302, 111<sup>th</sup> Cong. §107 (2010). For discussion of the privacy implications of such technologies, see Patrick R. Mueller, *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 (2006).

<sup>6</sup> <http://www.medicaldevice-network.com/features/feature81227> (last visited July 1, 2010).

<sup>7</sup> See Don Clark, *Take Two Digital Pills and Call Me in the Morning*, WALL ST. J. (Aug. 4, 2009).

<sup>8</sup> See <http://www.signonsandiego.com/news/2010/jul/28/sd-company-hopes-monitor-will-revolutionize/> (last visited August 1, 2010). Regular blood sugar monitors (which require pricking the finger) already exist to transmit such data electronically after each reading. See <http://www.ideallifeonline.com/products/glocomanager> (last visited July 20, 2010).

<sup>9</sup> See e.g., Upkar Varshney, *Pervasive Healthcare and Wireless Health Monitoring*, 12 MOBILE NETW. APPL. 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.").

<sup>10</sup> See <http://www.mybackgroundcheck.com> (last visited July 11, 2010).

<sup>11</sup> See <http://www.mybackgroundcheck.com/DrugTesting.aspx> (last visited July 11, 2010).

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 possible the low-cost sharing of verified personal information for economic reward, or, put differently, the incentivized extraction of previously unavailable personal information from individuals by firms. In this new world, economic actors do not always need to “sort” or screen each other based on publicly available information, but can instead 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 threat of data mining, aggregation and sorting that has preoccupied the burgeoning informational privacy field 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 disclose fully 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 do so 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 have the ability and incentive to disclose, all 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 evolves, privacy advocates must either concede defeat or focus on preventing unraveling. The latter will require both a theoretical shift in our conception of privacy harms and practical changes in privacy reform strategies.

The Article’s three Parts track these claims. Part I explores the emerging signaling economy.

\* \* \*

Part II takes up the Article’s second claim: that even the first steps we are now taking towards a signaling economy—steps like those in the three examples above—pose a new set of privacy challenges previously largely ignored.

Richard Posner first articulated these challenges decades ago, although at the time they were more theoretical than practical.<sup>12</sup> Even with control over her personal information, he argued, an individual will often

---

<sup>12</sup> Posner’s description of this problem is in Posner, *Privacy*, *supra* note \_\_ at 105-107. He began to develop such themes in RICHARD A. POSNER, *THE ECONOMICS OF JUSTICE* 234 (1981).

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, the economic “unraveling effect” will occur: in equilibrium, *all* will disclose their information, whether positive or negative, as 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.<sup>13</sup> 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 can't be more than one hundred oranges.

The unraveling effect posits that all sellers will fully disclose the number of oranges in the crate, regardless of how many their crate contains. Begin with the choice faced by a seller with one hundred oranges in his crate. If the seller stays silent, the buyer will assume 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. The silent seller gets pooled with all the lower-value sellers, 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, “[s]ilence cannot be sustained because high-value sellers will distinguish themselves from low-value sellers through voluntary disclosure.”<sup>14</sup> The economist Robert Frank coined the term the “full disclosure principle” to describe this phenomenon in his classic text *Passions Within Reason*. The principle is simple: “if some individuals stand to benefit by revealing a favorable value of some trait, others will be forced to disclose their less favorable values.”<sup>15</sup>

In the decades since Posner's challenge, however, privacy law has almost entirely overlooked the threat of unraveling. Instead, recent

---

<sup>13</sup> 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. See DOUGLAS G. BAIRD ET AL., *GAME THEORY AND THE LAW* 90 (1994) (using this example) [hereinafter BAIRD ET AL., *GAME THEORY*]; Robert H. Gertner, *Disclosure and Unraveling*, 1 THE NEW PALGRAVE DICTIONARY OF ECON. & THE LAW 605 (1998) (same).

<sup>14</sup> BAIRD ET AL., *GAME THEORY*, *supra* note \_\_ at 90.

<sup>15</sup> ROBERT H. FRANK, *PASSIONS WITHIN REASON* 104 (1988).

informational privacy scholarship<sup>16</sup> has focused on the privacy threats of firms sorting individuals by mining aggregated public data such as credit histories. Informational privacy law has reacted to sorting becoming more commonplace and sophisticated.<sup>17</sup> The field is dominated by Daniel Solove's concept of the "digital dossier," which is a metaphor for the aggregate of information available online about a given person.<sup>18</sup> Privacy scholars fear that we are moving towards a world in which everything becomes public—where all of our personal information becomes easily available to others as part of our digital dossier.<sup>19</sup> In reaction to this fear, the literature is replete with calls to give individuals greater control<sup>20</sup> over their personal information through the common law of property and tort and through stronger statutory privacy rights.<sup>21</sup>

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 they 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 discrimination. 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 as or more difficult a problem as data mining and the digital dossier.

\* \* \*

Part III thus begins to reorient informational privacy law towards the threats of signaling and unraveling.

---

<sup>16</sup> See Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087 (2006) (discussing the field of informational privacy law).

<sup>17</sup> See Part II(B) for discussion.

<sup>18</sup> See DANIEL J. SOLOVE, *THE DIGITAL PERSON 2* (2004) (defining the digital dossier).

<sup>19</sup> See 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); Corey 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); Lee Tien, *Privacy, Technology and Data Mining*, 30 OHIO N.U. L. REV. 389, 398-99 (2004) (explaining the risks digital dossiers pose to privacy and associational freedom).

<sup>20</sup> 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"), and the dominant prescribed remedy for privacy violation. See e.g., 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 legal protection for information privacy."); 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").

<sup>21</sup> See Part II(B).

\* \* \*

## I. THE PERSONAL PROSPECTUS & 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 how to determine whether your potential partner has such traits and isn't 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?<sup>22</sup>

These asymmetric information problems—how to distinguish one desirable “type” of person, good, or asset from another less desirable type—have occupied economists and legal scholars for decades. Consider the simple decision of whether to lend to Person A or Person B. If you could easily determine that A is more credit-worthy, you would choose to do business with A and not B (or, at least, to charge a greater interest rate to B than A). 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.<sup>23</sup> This creates extra costs for A and B, inefficiencies for you, and a burden on the economy generally.<sup>24</sup> If the market really falls apart, credit-worthy A types may be priced out of the market completely.<sup>25</sup>

Sorting and signaling are the two primary economic devices to overcome such information asymmetries.<sup>26</sup> Sorting or “screening” theory assumes that an uninformed party will filter counterparties based on what observable characteristics or information *are* available, if the desired characteristic is unobservable.<sup>27</sup> For example, a lender might use job turnover, prior bankruptcies, or a poor credit score as proxies for future default risk.

---

<sup>22</sup> See George A. Akerlof, *The Market for 'Lemons': Quality Uncertainty and the Market Mechanism*, 83 Q. J. ECON. 488 (1970).

<sup>23</sup> See generally Dwight M. Jaffee & Thomas Russell, *Imperfect Information, Uncertainty, and Credit Rationing*, 90 Q. J. ECON. 651, 651-52 (1976) (describing these dynamics).

<sup>24</sup> Joseph E. Stiglitz & Andrew Weiss, *Credit Rationing in Markets with Imperfect Information*, 72 AM. ECON. REV. 393 (1981).

<sup>25</sup> See Akerlof, *supra* note \_\_, at 490-92.

<sup>26</sup> For an overview of sorting and signaling, see John G. Riley, *Silver Signals: Twenty-Five Years of Screening and Signaling*, 39 J. ECON. LIT. 432 (2001).

<sup>27</sup> See e.g., Roger Klein, Richard Spady & Andrew Weiss, *Factors Affecting the Output and Quit Properties of Production Workers*, 58 REV. ECON. STUDIES 929 (1991) (exploring example of employers sorting job applicants based on high school graduation as a proxy for perseverance).

Signaling is the counterpart to sorting.<sup>28</sup> 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.”<sup>29</sup> Return to our credit example. If there are two types of borrowers—A & B—seeking funds and A is likely to pay back while B is not, A has incentive to reveal its type to the lender in order to receive a lower interest rate.

A may try to signal its type by simply saying “I am a good credit risk—I will repay my loans,” but talk is cheap.<sup>30</sup> The lender will doubt A because A has every reason to lie. Moreover, because it is easy to say such words, both A and B will say them and the lender will be no better off than it was before in trying to distinguish A from B.

A may therefore disclose information that can be used as a proxy of future creditworthiness, such as income level or employment history. For such disclosure to be an effective signal, however, the disclosed information must be verifiable. Such verification has been costly in an economy based on analog information.<sup>31</sup> An economic actor seeking to rely on a piece of information must expend time and resources to verify it—by calling references, checking employment or tax records, or calling to verify educational achievements. Although such steps are effective in some instances, they impose costs. When signaling is cost-prohibitive, economic actors will instead rely on sorting.

## B. SORTING AND THE DIGITAL DOSSIER

---

<sup>28</sup> 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.”).

<sup>29</sup> N. GREGORY MANKIW, *PRINCIPLES OF ECONOMICS* 482 (2004). 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 (2003).

<sup>30</sup> See Joseph Farrell & Matthew Rabin, *Cheap Talk*, 10 J. ECON. PERSP. 103 (1996) (discussing cheap talk generally).

<sup>31</sup> As a result, economists generally focus on signaling devices that are self-verifying by being costly to fake—whereby an action taken by A serves in and of itself as a signal of A’s type. See N. GREGORY MANKIW, *PRINCIPLES OF ECONOMICS* 482 (2004) (defining signaling). There are many examples. See e.g., DIANE COYLE, *THE SOULFUL SCIENCE: WHAT ECONOMISTS REALLY DO AND WHY IT MATTERS* 153 (2007) (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 STUDIES J. 35, 39 (1997) (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, 238 (1994) (an insured chooses a high-deductible health insurance plan, thereby signaling their belief in their health and their low risk to the insurance company). Spence began modern signaling theory with Michael Spence, *Job Market Signaling*, 87 Q. J. ECON. 355 (1973). See also A. 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).

This has been the situation in the “sorting economy” that has developed over the last one hundred and fifty years. 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.

\* \* \*

By the 1970s and 1980s, computer technology made it far easier for credit agencies to collaborate across geographic distances by sharing information, giving rise to the small number of large credit agencies that now dominate the American market.<sup>32</sup> 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 dossier.<sup>33</sup> “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.”<sup>34</sup> 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.<sup>35</sup> Supermarkets, airlines, hotels, and merchants all track and share information about consumers to better market their products.<sup>36</sup> 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.<sup>37</sup> In other words, sorting. As Douglas Baird has argued about lenders, for example,

---

<sup>32</sup> 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, leading to consolidation of the credit agency industry and the arrival of a few large, national credit agencies. *See* Pagano & Jappelli, *supra* at 1712 (“From a network of local monopolies, credit bureaus began to evolve into a nationwide oligopoly.”).

<sup>33</sup> 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 poses serious risks to privacy. For discussion of governmental use of such data, see e.g., 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).

<sup>34</sup> LAWRENCE LESSIG, CODE: VERSION 2.0 219 (2006).

<sup>35</sup> 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 (Kerr, Steeves & Lucock, eds., 2009). *See also* James X. Dempsey & Lara Flynn, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1464-65 (2004) (surveying the increase in data collection and data mining).

<sup>36</sup> *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 led corporations to data-collection efforts).

<sup>37</sup> *See* Millar, *supra* note \_\_\_ at 106 (discussing descriptive versus predictive data mining).

[a]dvances 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.<sup>38</sup>

Beyond credit markets, corporations might explore correlations between past consumer behavior (e.g., has this person bought both Brand X and Brand Y) and future purchases (e.g., will that predict that they will also purchase Brand Z).<sup>39</sup> An insurance company might use health records to predict life expectancy.<sup>40</sup> An employer might try to extrapolate the likelihood of future success as an employee from the tea leaves of a candidate's past.<sup>41</sup> A merchant might try to predict whether a given customer's check will bounce based on rudimentary information about that check-writer.<sup>42</sup>

The point is that the digital dossier is the technological culmination of one hundred and 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 to privacy.

---

<sup>38</sup> Douglas G. Baird, *Technology, Information, and Bankruptcy*, 2007 U. ILL. L. REV. 305, 312.

<sup>39</sup> See 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); JOSEPH P. BIGUS, *DATA MINING WITH NEURAL NETWORKS* 17-18 (1996) (discussing correlation of product purchases).

<sup>40</sup> 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.").

<sup>41</sup> The U.S. market for pre-employment background screening is roughly \$2 billion per year. See J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 76 U. CHI. L. REV. 109, 110 (2008). This 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).

<sup>42</sup> A merchant can electronically submit a shopper's drivers 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, 1632-1633 (2001) (discussing check verification systems).

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.<sup>43</sup>

This has been the dominant concern of the privacy field for the last decade.<sup>44</sup>

### 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—Tom Goodwin's 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 world in which firms can increasingly rely on information transmitted directly from a consumer to the firm rather

---

<sup>43</sup> DANIEL J. SOLOVE, *THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET* 17 (2007).

<sup>44</sup> See e.g. SIMSON GARFINKEL, *DATABASE NATION: THE DEATH OF PRIVACY IN THE 21<sup>ST</sup> CENTURY* (2001) (discussing the threat of linked databases and the digitization of records); 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, 10 (2000) (discussing how these technologies allow for collection of "vast amounts of in-depth, and potentially sensitive, personal information"); H.T. Tavani, *Informational Privacy, Data Mining, and the Internet*, 1 ETHICS & INFORMATION TECHNOLOGY 37 (1999); Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435 (2008) (discussing the end of "practical obscurity" brought about by data mining); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317 (2008) (discussing widespread use of data mining by government agencies and government's reliance on commercial data gathering companies); Tal Z. Zarsky, "Mine Your Own Business!": *Making the Case for the Implications of Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE J.L. & TECH. 4 (2002-2003) (discussing privacy concerns related to data mining); William Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 291 (2003) (noting "three major digital developments that 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").

than engage in data mining to “read the tea leaves” about the consumer’s characteristics or behavior.

The personal prospectus is a metaphor to represent the core idea that such signaling is becoming increasingly pervasive, cost-effective, and powerful as an economic mechanism. This section explores this 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 signaling will thus continue to become more and more important and ubiquitous as a response to information asymmetries.<sup>45</sup> This is a novel and somewhat radical claim. Understanding it sets the groundwork for Part II, which turns to the implications of these developments for informational privacy law.

The key change causing the shift from the sorting economy to the signaling economy is that digital information can be verified at very low cost. This change is occurring—and will occur—in at least two domains: *digital monitoring* of directly observable data and *digital access* to directly verifiable data.

\* \* \*

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 and will play an important role in the evolution of a signaling economy.

*i. Digital Monitoring of Directly Observable Data*

Monitoring and sensor technology is increasingly sophisticated and pervasive. The data collected by such sensors are often extremely personal, but also extremely valuable as part of an individual’s personal prospectus. We are now able to track, record, and share vastly more and better information about ourselves, and the technologies making such sharing and signaling possible 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.<sup>46</sup>

---

<sup>45</sup> I do not claim that signaling will eclipse sorting, nor that the digital dossier and the threat of sorting will be less important than the threats of signaling. I merely wish to argue that signaling is increasing as the costs of signaling drop, and that this will change our understanding of informational privacy.

<sup>46</sup> In addition to the monitoring technologies discussed here, I have excluded others for brevity. Smart grid technologies offer many similar monitoring and signaling opportunities. See Elias L. Quinn, *Privacy and the New Energy Infrastructure*, available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1370731](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370731) (last visited July 28, 2010); Patrick McDaniel & Stephen McLaughlin, *Security and Privacy Challenges in the Smart*

Remote health monitoring, or pervasive healthcare, is a hot technology as ubiquitous Internet access makes constant, real time sensors possible.<sup>47</sup> Such monitoring is touted as a means to improve care and reduce health care costs.<sup>48</sup> Remote monitoring systems can track weight loss,<sup>49</sup> blood glucose levels,<sup>50</sup> arrhythmia (irregular heart contractions),<sup>51</sup> epilepsy,<sup>52</sup> stress,<sup>53</sup> and vital signs such as temperature, heart rate and respiration.<sup>54</sup> Intel is developing a “magic carpet” for elders that tracks a homeowner’s movements in order to gather data to prevent falls, a major component of health costs for seniors.<sup>55</sup> Newer systems are also being imagined to remotely monitor the condition of mental health patients. These systems would track sleep pattern, weight loss or gain, physical movement, vital signs and medication compliance to produce alerts for worsening mental illness.<sup>56</sup>

Individuals will increasingly be 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 micro-payments to reward a user’s exercise or healthy eating.<sup>57</sup> Employers have already begun to incentivize employees to participate in wellness programs or to meet health goals for blood pressure, cholesterol levels or weight.<sup>58</sup> Some have tracked employees’ smoking habits, including when the employees are away

---

*Grid*, IEEE SECURITY & PRIVACY (May/June 2009) (“Energy use information stored at the meter and distributed thereafter acts as an information-rich side channel, exposing customer habits and behaviors.”).

<sup>47</sup> For an overview of this field, see Upkar Varshney, *Pervasive Healthcare and Wireless Health Monitoring*, 12 MOBILE NETW. APPL. 113, 115 (2007) (“Comprehensive health monitoring services would allow patients to be monitored at any time in any location.”).

<sup>48</sup> See e.g., Upkar Varshney, *A framework for supporting emergency messages in wireless patient monitoring*, 45 DECISION SUPPORT SYSTEMS 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.”).

<sup>49</sup> See <http://www.bodymedia.com> (last visited July 10, 2010).

<sup>50</sup> See <http://www.ideallifeonline.com> (last visited July 10, 2010).

<sup>51</sup> See <http://www.corventis.com> (last visited July 10, 2010).

<sup>52</sup> See S. Modarreszadeh, *Wireless, 32-Channel, EEG and epilepsy monitoring system*, Proc. 19<sup>th</sup> Annual IEEE Intl. Conf. on Eng. In Med. And Bio (1997).

<sup>53</sup> See E. Jovanov et al., *Stress monitoring using a distributed wireless intelligent sensor system*, 3 IEEE Engineering in Medicine and Biology Magazine 22 (2003).

<sup>54</sup> See <http://www.toumaz.com> (last visited July 10, 2010) (developing a “wearable plaster” that tracks vital signs).

<sup>55</sup> See Clark, *supra* note \_\_\_.

<sup>56</sup> See Upkar Varshney, *A framework for wireless monitoring of mental health conditions*, 31<sup>st</sup> Ann. Intl. Conf. of IEEE (Sep. 2-6, 2009), available at <http://www.ieeeexplore.org>.

<sup>57</sup> See Upkar Varshney, *Pervasive Healthcare and Wireless Health Monitoring*, 12 MOBILE NETW. APPL. 113, 115 (2007).

<sup>58</sup> Safeway grocers, 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 Initiatives*, N. ENGL. J. MED. 362, 362 (2010) (discussing Safeway program).

from their place of work.<sup>59</sup> Some have fired employees who engage in behavior likely to raise the employer's health insurance costs.<sup>60</sup>

Most dramatically, Congress recently endorsed incentive-based health reform in the health care bill.<sup>61</sup> Although generally group health plans cannot discriminate based on health status, the PPACA permits employers to provide discounts, rebates and rewards for those who participate in wellness initiatives.

\* \* \*

Given this foundation, it is quite easy to imagine individuals or employees seeking to 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. Recent court cases in Connecticut<sup>62</sup> and California<sup>63</sup> have raised issues 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, 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 ...."<sup>64</sup> In addition, at least three states<sup>65</sup> have

---

<sup>59</sup> See Jeremy W. Peters, *Company's Smoking Ban Means Off Hours, Too* (Feb. 8, 2005), available at <http://www.nytimes.com/2005/02/08> (last visited July 26, 2010).

<sup>60</sup> Jill Schachner Channen, *The Boss is Watching* (Jan. 1, 2008), available at <http://abajournal.com> (last visited July 5, 2010).

<sup>61</sup> The PPACA codifies the incentive regulations previously established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). For an overview of these changes, see U.S. CHAMBER OF COMMERCE, *CRITICAL EMPLOYER ISSUES IN THE PATIENT PROTECTION AND AFFORDABLE HEALTH CARE ACT 29* (2010).

<sup>62</sup> In *American Car Rental, Inc. v. Commissioner of Consumer Protection*, the State of Connecticut filed an administrative complaint against a car rental agency that charged a \$150 fee each time a customer's rental vehicle exceeded seventy-five miles per hour for more than two consecutive minutes. *American Car Rental, Inc. v. Commissioner of Consumer Protection*, 273 Conn. 296, 869 A.2d 1198 (2005). The rental agreement warned customers that the agency's cars were "GPS equipped" and that the \$150 fee would apply, but did not explain GPS technology or provide detail about the workings of the fee. 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.

<sup>63</sup> In *People v. Accelaron Corp.*, the State of 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 *People v. Accelaron Corp.*, available at [http://ag.ca.gov/newsalerts/cms04/04-129\\_complaint.pdf](http://ag.ca.gov/newsalerts/cms04/04-129_complaint.pdf) (last visited July 23, 2010).

<sup>64</sup> 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 (2007).

enacted statutes restricting the use of such monitors.<sup>66</sup> California and New York, for example, prohibit 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.<sup>67</sup>

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 action would have resulted. No state has addressed directly the consumer's potential *interest* in sharing GPS-enabled information about her use of a rental vehicle in order to receive a discount. The car insurance examples in the Introduction suggest, however, 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.

\* \* \*

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 their quality 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. John Halpin*,<sup>68</sup> 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. 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.<sup>69</sup>

---

<sup>65</sup> See Conn. Gen. Stat. § 42a-9-609 (2003); Cal. Civ. Code § 1936(6)(o) (2002); N.Y. Gen. Bus. Law § 20 Art. 26 § 396-z (2006).

<sup>66</sup> 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, nor banned consumers from disclosing such information as they see fit. See Altaras, *supra* note \_\_ at 8 (discussing state legislation).

<sup>67</sup> Cal. Civ. Code § 1936(6)(o) (2002).

<sup>68</sup> Dep't of Education v. Halpin, New York City Office of Administrative Trials and Hearings, OATH Index No. 818/07 (Aug. 9, 2007).

<sup>69</sup> For additional discussion, see Jeremy Gruber, *RFID and Workplace Privacy*, [http://www.workrights.org/issue\\_electronic/RFIDWorkplacePrivacy.html#\\_ftn15](http://www.workrights.org/issue_electronic/RFIDWorkplacePrivacy.html#_ftn15) (last visited July 28, 2010); Novitech Now Using Active RFID System for Employee Monitoring (Aug. 28, 2010) <http://www.rfidnews.org/2007/08/28/novitech-now-using-active-rfid-system-for-employee-monitoring> (last visited July 28, 2010).

Such employee tracking will likely increase if radio frequency identification (RFID) becomes more ubiquitous. RFID tags have been used to track employees as they move around a factory floor or come and go in health care settings.<sup>70</sup> The Dubai International Airport uses RFID tags to track over nine thousand workers, the security firm CityWatcher is experimenting with subcutaneous RFID tags injected into the forearms of security guards, and the Oak Ridge National Laboratories in Tennessee uses RFID to monitor whether employees have properly evacuated in emergency situations.<sup>71</sup>

\* \* \*

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.

*ii. 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 as or more 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.<sup>72</sup> 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

<sup>70</sup> See <http://www.rfidnews.org/2007/08/now-using-active-rfid-system-for-employee-monitoring> (last visited July 20, 2010); [http://www.contactlessnews.com/time-employee-tracking-helps-home-caregivers?tag=Time\\_and\\_Attendance](http://www.contactlessnews.com/time-employee-tracking-helps-home-caregivers?tag=Time_and_Attendance) (last visited July 10, 2010).

<sup>71</sup> These examples are drawn from Marisa Anne Pagnattaro, *Getting Under Your Skin—Literally: RFID in the Employment Context*, 2008 J.L. TECH. & POL'Y 237, 242-43.

<sup>72</sup> 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 (summarizing Fair Credit Reporting Act, the Privacy Act, and the limits of U.S. privacy law).

Google Health. In addition, many important facts about us are kept in digital databases to which we don't 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, the court system holds documentation of my criminal and legal history (if I have one).

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, one will be able to digitally link an interested counterpart to these sources that hold *verified* evidence about oneself. 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.<sup>73</sup> Your employer's computer will simply issue a verification of the requested information—"yes, she does indeed make \$100,000."

Rather than a resume, individuals will grant access to their personal prospectus, and thus access to the underlying verified data to which a resume typically attests. Employment history will be verified as employers (or the Internal Revenue Service) feed data out in response to authorized queries about an individual's work record. Criminal history will be verified as court clerks feed data out in response to authorized queries about an individual's past. Medical records will be verified as physicians, hospitals and insurance companies feed data out 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 underlying 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

---

<sup>73</sup> 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 progenitor of 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 Jonathan Zittrain, *Privacy 2.0*, 2008 U. CHI LEGAL F. 65, 107-108 (discussing Nelson's original vision and current debate on the issue). The personal prospectus is a somewhat different, but related, idea. Rather than focus on authorial content shared over the web—such as a book or photograph—I am focused on data about a person that originally resides in an institution's database but is then released onto the web and winds up in the digital dossier.

portable, comparable, and verifiable, an individual will be able to present him or herself to others through the personal prospectus—to show his or her type, characteristics, and history by revealing verified information about himself.

The personal prospectus will thus differ from today's digital dossier in two primary ways.<sup>74</sup> First, the prospectus will be comprised of *verified* information, whereas the digital dossier is largely comprised of unverified 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 from which it was originally issued. The prospectus would not only contain an educational transcript, but 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 other's 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.

\* \* \*

*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.* If John was 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 that debt. He could

---

<sup>74</sup> 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 likely to regulate their behavior going forward.

reveal his credit card transactions for the last three years, showing his record of paying his debts timely 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 John 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 as some individuals initially find it in their interest to disclose information for personal gain and then, as the unraveling proceeds, all realize that disclosure is no longer a choice but instead a necessity as the signaling economy attaches stigma to staying silent.

\* \* \*

### A. UNRAVELING IN A SIGNALING ECONOMY

As low-cost signaling evolves and becomes more ubiquitous, the first and most fundamental point is that some will want to disclose and some will not. All 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 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 will gain in all contexts. 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.

#### *i. Self-Interested Self-Disclosure & Defending Against the Digital Dossier*

Simple self interest will drive self-disclosure by those with positive private information. Assuming one has positive characteristics to share, revealing them can provide economic benefits. This is what the car insurance, health monitoring and employment tracking examples used to this point illustrate: individuals seeking preferential treatment or discounts in return for disclosing information useful to other economic actors transacting across an information asymmetry.

Although most privacy literature has focused on how we can and should keep information to ourselves, this ignores the reality that in many cases it is extremely valuable to share information about oneself with others.<sup>75</sup> The privacy field has been so concerned with the downsides of sorting that it has overlooked that many will at least initially perceive upsides to increased signaling. If one is a healthy, non-smoking, regular exerciser, a means to credibly signal that to one's medical insurer will mean lower premiums. If one is a dependable, income-earning employee, a means to credibly signal that to one's bank will mean lower rates. If one has a large bank account and a string of other assets, a means to credibly signal that to a luxury store will mean better service.<sup>76</sup>

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—that although you are a “good” borrower or a low-risk insured, you will be incorrectly sorted into the wrong category. Signaling via the personal prospectus can correct the inaccuracies of the dossier.

\* \* \*

## ii. *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 that 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 there is information to hide. 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<sup>77</sup> and Sanford Grossman<sup>78</sup> independently explored

---

<sup>75</sup> 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).

<sup>76</sup> See Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1049-1050 (1999) (discussing the ways in which self-disclosure can reduce search costs).

<sup>77</sup> See Paul R. Milgrom, *Good news and bad news: representation theorems and applications*, 12 BELL J. OF ECON. 380, 388 (1981) (discussing salesman's incentive to fully disclose product quality because of similar unraveling effect).

<sup>78</sup> See Sanford J. Grossman, *The informational role of warranties and private disclosure about product quality*, 24 J. LAW AND ECON. 461 (1981); S.J. Grossman & O.D. Hart, *Disclosure Laws and Takeover Bids*, 35 J. OF FIN. 323, 323 (1980) (“[I]f there is no

the unraveling process that occurs as those that can certify their quality do so in order to distinguish themselves from the larger pool of lower grade labor, products, or services.<sup>79</sup> 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, pre-trial settlement, etc.).<sup>80</sup>

The unraveling effect holds that under conditions of information asymmetry but with verifiable information and penalties for fraud,<sup>81</sup> 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, and thus 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 Frank puts it, “[t]he 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. . . . 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.”<sup>82</sup>

In a signaling economy, consumers may increasingly pay a price for keeping personal information private. This differs from price discrimination or weblining, because in those instances a firm is sorting a consumer based on the consumer’s known (or supposed) characteristics derived from

---

transactions cost then it will always be in the seller’s interest to disclose the quality of [an] item voluntarily.”)

<sup>79</sup> 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. OF 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* 134 (1983) (discussing unraveling).

<sup>80</sup> See e.g., Andrew E. Stivers, *Unraveling of Information: Competition and Uncertainty*, 4 TOPICS IN THEOR. ECON. 1 (2004) (finding that increased competition in market increases unraveling effect); Ronald A. Dye & Sri S. Sridhar, *Industry-Wide Disclosure Dynamics*, 33 J. OF ACCT. RES. 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 RONALD E. GRIESON (ED.), *ANTITRUST AND REGULATION* 91 (1986). For early work on pre-trial settlement, see Steven Shavell, *Sharing of Information Prior to Settlement or Litigation*, 20 RAND J. OF ECON. 183 (1989).

<sup>81</sup> 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* (NBER Working Paper, Apr. 2009), available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1376153](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=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).

<sup>82</sup> FRANK, *PASSIONS WITHIN REASON*, *supra* note \_\_ at 106-108.

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.

\* \* \*

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 Richard Posner should claim that title, and a few others have taken up his connection between unraveling and privacy since.<sup>83</sup> As Posner put it, “[b]ecause 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.”<sup>84</sup>

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 *have* been “reasons unrelated to the private benefits of concealment” that have prevented unraveling to date: the general lack of technological means to build a robust signaling economy. It has been cheaper to sort than to rely on signals. That is changing, however, as we have seen. 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.

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

---

<sup>83</sup> Jessica Littman's early article on privacy as a property right saw the unraveling problem, for example. She notes that control is at best a stepping stone towards alienability. Most interesting, Littman 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.” See Jessica Littman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1301 (2000). See also Randal C. Picker, *Online Advertising, Identity and Privacy* (working paper), available at <http://ssrn.com/abstract=1428065> (last visited September 22, 2010) (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).

<sup>84</sup> Richard Posner, *Privacy*, *supra* note \_\_ at 107.

proposed solutions that seek to increase individual control over information. Control provides little protection from unraveling, however. 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.

*i. The Inadequacy of Control*

\* \* \*

[E]ven a cursory run through the literature by category should suffice to demonstrate that control dominates as the primary solution of privacy advocates.<sup>85</sup> For example, much informational privacy literature has focused on property-based prescriptions. The basic idea is that “privacy 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.”<sup>86</sup>

\* \* \*

Tort-based solutions similarly focus on control. Generally these scholars have bemoaned the inadequacy of existing tort remedies<sup>87</sup> and proposed additions or improvements to tort law to increase individual control.<sup>88</sup>

\* \* \*

Proposed legislative solutions also emphasize control rights. As Fred Cate has noted, “[v]irtually all privacy bills before Congress reflect this goal: ‘to strengthen control by consumers’ and ‘to provide greater individual control.’”<sup>89</sup> Prescriptive informational privacy scholarship follows this pattern.

\* \* \*

---

<sup>85</sup> See e.g., Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 820 (2000) (“The leading paradigm ... conceives of privacy as a personal right to control the use of one’s data.”).

<sup>86</sup> Jessica Littman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1287 (2000).

<sup>87</sup> 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).

<sup>88</sup> See 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).

<sup>89</sup> See FRED H. CATE, *PRIVACY IN PERSPECTIVE* 5 (2001).

I don't 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.<sup>90</sup> 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 required all to disclose.

\* \* \*

### III. UNRAVELING'S LIMITS & LIMITING UNRAVELING

Let us summarize the argument to this point. Verifiable signals theoretically lead to unraveling as a pooling equilibrium develops in which 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 through digital monitoring of directly observable data and digital access to directly verifiable data, however, thus requiring serious attention to the problem of privacy's unraveling.

This Part takes up this challenge. I do not advocate for a draft statute nor 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. At the same time, privacy advocates should be sobered by the rise of a signaling economy. The personal prospectus complicates informational privacy both in practice and in theory.

---

<sup>90</sup> See *supra* note \_\_ (discussing the private remainder).

## A. UNRAVELING'S LIMITS

One possible counterargument at this point could focus on the known limits of the unraveling effect. Not all information markets unravel, even when participants in those markets can verifiably signal at low cost. This Section explores what we know about the limits of the unraveling effect.<sup>91</sup> It may provide some reassurance for privacy advocates 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.

### i. Transaction Costs

Research shows that unraveling may be partial or incomplete when it is costly to disclose information,<sup>92</sup> costly to acquire it,<sup>93</sup> or difficult for the informed party to credibly communicate the information to her uninformed counterpart.<sup>94</sup> 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 no verifiable signals exist,<sup>95</sup> unraveling cannot occur.

A recent study of the online auto auction site eBay Motors demonstrated, for example, that “disclosure costs affect how much information the seller decides to post” in online auctions, and therefore the functioning of the market.<sup>96</sup> 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

---

<sup>91</sup> This Section reviews some of the main constraints on unraveling. For an overview including other constraints, see David Dranove & Ginger Z. Jin, *Quality Disclosure and Certification: Theory and Practice*, NBER Working Paper (Jan. 2010), available at SSRN: <http://ssrn.com/abstract=1537763>.

<sup>92</sup> See Boyan Jovanovic, *Truthful Disclosure of Information*, 13 BELL J. ECON. 36 (1982) (explaining that transaction costs inhibit the effect).

<sup>93</sup> See Joseph Farrell, *Voluntary Disclosure: Robustness of the Unraveling Result, and Comments on Its Importance*, in ANTITRUST AND REGULATION (RONALD E. GRIESON ED. 1986).

<sup>94</sup> See *e.g.*, Steven Shavell, *A Note on the Incentive to Reveal Information*, 14 GENEVA PAPERS ON RISK AND INSURANCE 66 (1989) (exploring distinction between unraveling with verifiable versus unverifiable information).

<sup>95</sup> It is worth noting that in some instances the lack of verifiability does not necessarily prevent unraveling. In some markets, early disclosures can get started by 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 INTL. 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).

<sup>96</sup> See Gregory Lewis, *Asymmetric Information, Adverse Selection and Online Disclosure: The Case of eBay Motors* (Jan. 11, 2010), available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1358341](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1358341) (last visited August 3, 2010).

unravels towards full disclosure—sellers disclose such pictures because it is low cost to do so, the photographic representation of the car is verifiable when the buyer takes possession, and therefore failing to post such photos is taken as a signal that there is something to hide.<sup>97</sup> The author notes that “where bandwidth and technology are available to [post] rich media such as photos and videos, adverse selection problems are mitigated.”<sup>98</sup> 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. As we’ve seen, health monitoring is an 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. In 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.

ii. *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 because the information type makes verifiability impossible. Okuno-Fujiwara, Postlewaite and Suzumura revealed this problem.<sup>99</sup> They explain 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.<sup>100</sup> 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 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, are there few oranges in the crate or is the seller merely ignorant of the number of oranges? This may lead to

---

<sup>97</sup> *Id.*

<sup>98</sup> *Id.*

<sup>99</sup> See Masahiro Okuno-Fujiwara, Andrew Postlewaite & Kotaro Suzumura, *Strategic Information Revelation*, 57 REV. OF ECON. STUDIES 25, 27 (1990) (“[O]ur paper emphasizes how restrictive are the conditions which guarantee the revelation of information in equilibrium.”).

<sup>100</sup> 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”).

a partial unraveling as those with “good” information disclose, but not a complete unraveling of all sellers’ information.<sup>101</sup>

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.<sup>102</sup> For example, restaurants have not typically disclosed 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 seller’s silence.<sup>103</sup>

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<sup>104</sup> 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.

*iii. Inability to Accurately Infer a Negative*

Other constraints may have greater impact on privacy’s unraveling. One constraint is whether the uninformed can accurately draw negative inferences from nondisclosure. Michael Fishman and Kathleen Haggerty’s work has shown, for example, that for unraveling to occur the uninformed

---

<sup>101</sup> See BAIRD ET AL., GAME THEORY, *supra* note \_\_ 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.”).

<sup>102</sup> 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 decisionmaker’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*”).

<sup>103</sup> 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”).

<sup>104</sup> See BAIRD ET AL., GAME THEORY, *supra* note \_\_ 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 that the player knows it; and so forth.”).

receiver of signaled information must be able to understand the disclosed information and actually draw negative inferences from nondisclosure.<sup>105</sup> If consumers do not draw negative inferences from silence, sellers have no incentive to disclose product information.<sup>106</sup> Some have suggested that this explains the failure of most hospitals to disclose evaluations of their quality—patients seem to naively believe that their doctors are above average even without disclosure, and therefore unraveling does not get started.<sup>107</sup> More generally, unsophisticated actors may not think strategically and may be naively credulous. If informed sellers believe this, for example, they will fail to disclose, treating every buyer as if he is unsophisticated.<sup>108</sup> Only when all (or most) uninformed parties in a market are sophisticated players will the unraveling effect occur and force disclosure by informed parties.

\* \* \*

*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 there is none of the nutrient present.

These results suggest that privacy's unraveling through the personal prospectus may be less than complete. Even if those with the very best traits disclose fully, all may not 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 at exactly what point 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. (Note, of course, that they will still be lumped together with the others at the bottom of the particular quality spectrum.)

---

<sup>105</sup> See Michael J. Fishman & Kathleen M. Haggerty, *Mandatory Versus Voluntary Disclosure in Markets with Informed and Uninformed Customers*, 19 J.L. ECON. & ORG. 45 (2003).

<sup>106</sup> See 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); 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).

<sup>107</sup> See DAVID DRAVNOVE, CODE RED (2008) (calling this the “Lake Woebegone effect”).

<sup>108</sup> See Paul Milgrom & John Roberts, *Relying on the information of interested parties*, 17 RAND J. ECON. 18, 20 (1986) (“[A] rational salesman will treat every buyer as if he were naively credulous.”).

This is relatively little consolation, however. In many of the examples discussed here, the uninformed players are homogenous 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, and they seek positive information about health characteristics or behaviors that is not subject to Mathios' boundedness problem (e.g., does a given insured smoke?). 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.

*iv. Norms*

Finally, sometimes privacy norms develop that constrain unraveling. 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.<sup>109</sup> In equilibrium, everyone should become a nudist. This is not, of course, the case. The norm against nudity prevents disclosure. It could have developed for many reasons, including the potential inefficiencies of widespread nudity. The point, however, is simply that in some cases informal norms prevent unraveling.

A recent study of SAT score disclosure by college applicants seems to support this 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 80,000 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.<sup>110</sup> 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.

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

---

<sup>109</sup> See Posner, *Privacy*, *supra* note \_\_ at 107 (discussing this example).

<sup>110</sup> See Gabrielle Chapman & Michael Conlin, *The Economics of Voluntary Disclosure in SAT Scores*, available at <https://www.msu.edu/~dickerc/301f06/SAT.pdf>.

benefits, as this 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.<sup>111</sup> 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.

B. LIMITING UNRAVELING: COMPARING REGULATORY STRATEGIES TO PRESERVE 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 available legal constraints that might prevent unraveling.

i. *Don't Ask, Don't Tell?*<sup>112</sup>

Inquiry limits and disclosure limits—don't ask rules and don't tell rules—are often employed to protect personally or socially sensitive information.<sup>113</sup> Inquiry limits forbid an uninformed party from seeking

---

<sup>111</sup> 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).

<sup>112</sup> 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. Miller and Gao propose that Presidents and public officials could 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 e.g., James D. Miller & Lixin Gao, *Creating a Subpoena-Proof Diary: A Technological Solution to a Legal Problem*, 3 J. INFO., L. & TECH. (2001), available at [http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001\\_3/miller](http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/miller) (last visited August 1, 2010).

<sup>113</sup> The most infamous example of a “don't ask, don't tell” policy is the military's stance towards homosexual and bisexual service members. See 10 U.S.C. § 654. This policy is not a response to the threat of unraveling information disclosure.

information from an informed counterpart.<sup>114</sup> For example, the Americans With Disabilities Act (ADA) bars an employer from asking a potential employee about disabilities,<sup>115</sup> 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.<sup>116</sup>

Inquiry limits rarely seem to inhibit unraveling, however.<sup>117</sup> Economists have long recognized that the unraveling effect will typically render an inquiry limit ineffective. Robert Frank considers the problem of employment discrimination regulations:

“Consider ... legislation that prohibits employers from asking about marital status and plans for having children. ... It is not sufficient merely to prohibit employers from asking about demographic categories. For if a woman realizes that her own particular categories place her in the most favored hiring category, she has every incentive to volunteer information about them. 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.”<sup>118</sup>

This sort of unraveling is exactly what one finds in most job markets. Empirical examination of resumes shows that job candidates very often reveal information to potential employers that they need not, most likely in order to signal traits that they perceive will assist them in their quest for employment.<sup>119</sup>

Given this problem, there are contexts in which we deploy disclosure limits. We forbid bank examiners from discussing bank examinations publicly, for example, for fear that unraveling will weaken the

---

<sup>114</sup> Robert H. Gertner, *Disclosure and Unraveling*, in 1 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 605, 605 (1998) (“Inquiry limits are legal rules that try to restrict the ability of an uninformed party to ask for disclosure from informed parties.”).

<sup>115</sup> See 42 U.S.C. § 12112(c)(2)(A).

<sup>116</sup> See BAIRD ET AL., GAME THEORY, *supra* note \_\_ at 92 (discussing these examples).

<sup>117</sup> See BAIRD ET AL., GAME THEORY, *supra* note \_\_ at 92 (“Inquiry limits ... may be ineffective unless there is some mechanism that prevents voluntary disclosure of the information.”).

<sup>118</sup> ROBERT H. FRANK, PASSIONS WITHIN REASON 107 (1988).

<sup>119</sup> See e.g., Lynne Bennington & Ruth Wein, *Aiding and Abetting Employer Discrimination: The Job Applicant’s Role*, 14 EPL. RESPONSIBILITIES & RIGHTS 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).

banking system when it is already under stress.<sup>120</sup> The unraveling problem is obvious: banks with good reports would want to disclose their relative health; the public will run to those banks; this will damage other relatively 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. Individuals, by contrast, are unused to such micro-managing 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 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.<sup>121</sup> 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 early decision, because the binding early decision process prevents them from comparing financial aid packages across different universities after their admission. 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.

---

<sup>120</sup> See BAIRD ET AL., *GAME THEORY*, *supra* note \_\_ at 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.").

<sup>121</sup> 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).

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

ii. *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 decision-maker 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.<sup>122</sup> The Fair Credit Reporting Act<sup>123</sup> bars creditors from inquiring about or denying credit on the basis of bankruptcies more than ten years old.<sup>124</sup> As discussed in Part I, some states have limited car rental companies from using data from GPS monitors to penalize consumers.<sup>125</sup> And our health care statutes limit an insurer’s use of information about an insured’s medical condition when the insurer is setting coverage or premiums.<sup>126</sup>

More recently, Congress has enacted a powerful “don’t use” rule to prevent information unraveling in the context of genetic discrimination.<sup>127</sup> Individuals in possession of positive 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. “Under these circumstances, silence conveys information.”<sup>128</sup> Although some scholars have advocated for the efficiencies of total disclosure,<sup>129</sup> 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

---

<sup>122</sup> See *Carter v. Kentucky*, 450 U.S. 288 (1981). For discussion of this example in the context of unraveling, see Robert H. Gertner, *Disclosure and Unraveling*, in 1 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 605, 605 (1998).

<sup>123</sup> 15 U.S.C. § 1681 et seq.

<sup>124</sup> See *id.* § 605(a)(1). See also RICHARD A. POSNER, *OVERCOMING LAW* 300 (1995) (discussing this example).

<sup>125</sup> See *supra* notes \_\_\_-\_\_\_ and accompanying text.

<sup>126</sup> See *supra* notes \_\_\_-\_\_\_ and accompanying text.

<sup>127</sup> See Sagit Ziskind, *The Genetic Information Nondiscrimination Act: A New Look at an Old Problem*, 35 RUTGERS COMP. & 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).

<sup>128</sup> *Id.* at 198.

<sup>129</sup> 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.”).

decisions.<sup>130</sup> The 2008 Genetic Information Nondiscrimination Act (GINA) is one example. GINA bars the use of genetic information by insurers to prevent unraveling.<sup>131</sup>

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, that use should be forbidden because of some social harm greater than the social benefits of 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.

#### C. PUBLIC CHOICE PROBLEMS, OR IF WE CAN'T EVEN ENACT CONTROL RIGHTS, HOW CAN WE LIMIT 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?

\* \* \*

#### CONCLUSION

The economy is changing, and privacy law must change as well. I do not have easy prescriptions to offer—my purpose has been more descriptive than normative. But it is clear that for the field of informational privacy law to remain relevant, it must address the unraveling problem that has to this point been merely a theoretical curiosity. The dominant syllogism in privacy theory must give way to new ways to conceive of privacy interests, and new arguments about why unchecked signaling should be considered a harm. If privacy advocates fear a full disclosure future, they must articulate why. In a signaling economy, they will face even *more* organized opposition to restricting information disclosure than they have

---

<sup>130</sup> See Ziskind, *supra* note \_\_ at 200 (“The best practical solution is ... comprehensive protection against health insurers’ use of genetic information ....”).

<sup>131</sup> See GINA, Pub. L. No. 110-233, 122 Stat. 881.

faced to date. Their task, in short, is becoming harder, not easier, as the personal prospectus grows, the signaling economy evolves, and privacy's unraveling continues.