

## Chicago-Kent College of Law

---

From the Selected Works of Richard Warner

---

Fall 2014

# Self, Privacy, and Power: Is It All Over? (with R. Sloan)

Richard Warner

# Self, Privacy, and Power: Is It All Over?

Richard Warner\* and Robert H. Sloan\*\*

I. THE SELF AND SOCIAL ROLES .....	4
A. The Concept of Privacy in Public .....	5
B. The Ideal of a Multifaceted Self.....	7
C. Social Roles.....	8
D. The Need for Privacy in Public.....	10
II. INFORMATIONAL NORMS AND THE CREATION OF PRIVACY IN PUBLIC.....	14
A. Informational Norms .....	14
B. Collection: Constraints on Merely Knowing .....	16
C. Use: The Allocation of Risks and Benefits .....	18
D. Distribution: The Multiplier .....	20
E. The Power Shift and the Tradeoff Challenge.....	22
III. NORMS AND COORDINATION .....	24
A. Coordination Norms.....	25
B. Value-Optimality and Privacy in Public .....	26
IV. THE EROSION OF PRIVACY IN PUBLIC: THE LOSS OF VALUE-OPTIMALITY.....	28
A. Collection: Anybody Can Know About Anybody .....	29
B. Allocation of Risks and Benefits.....	33
C. Distribution.....	38
D. Two Ways to “Play Without a Helmet” .....	43
V. THE EROSION OF PRIVACY IN PUBLIC: LACK OF NORMS .....	44
A. No Shared Conception of Role Appropriateness .....	45
B. A Similar Four-Part Pattern .....	46
C. What Is To Be Done?.....	49
VI. IS IT ALL OVER?.....	51
A. A Tragedy of the Commons.....	51
B. Values.....	54
C. The Need for Trust .....	55
VII. A WORRIED AFTERTHOUGHT .....	56

Informational privacy is the ability to determine what others do with your information.<sup>1</sup>

Small towns are notorious for their lack of informational privacy:

---

\* Professor of Law, Chicago-Kent College of Law, Visiting Foreign Professor, University of Gdańsk, Poland.

\*\* Professor and Head, Department of Computer Science, University of Illinois at Chicago. Partially supported by National Science Foundation Grant No. DGE-1069311.

<sup>1</sup> ALAN WESTIN, *PRIVACY AND FREEDOM* 7 (1967). *See also* JAMES B. RULE, *PRIVACY IN PERIL: HOW WE ARE SACRIFICING A FUNDAMENTAL RIGHT IN EXCHANGE FOR SECURITY AND CONVENIENCE* 3 (2007) (defining privacy “as the exercise of an authentic option to withhold information on oneself”);

I live in a small town. We have about 11,000 inhabitants. Everyone knows me. We all know each other. When I ask my neighbour, if my best friend that lives on the other side of the town has a girlfriend, I will get the answer. However it will not be just a “yes” or “no” answer - I will get to know everything about her. Her name, age, what her parents do, her school, every single detail, and that is the disadvantage of our little town.<sup>2</sup>

Cities offer greater privacy, a fact that impressed the great nineteenth century sociologist, Georg Simmel. Simmel emphasized that increased privacy meant increased freedom from interference and censure and hence greater opportunity for the development of a multifaceted self:

whereas earlier [in small communities], individuality was determined primarily by belonging to a single group, it is now [in large cities] formed by the *combination* of the diverse groups to which the person belongs . . . Someone could belong to various professional associations, at the same time as he belongs to a scientific society, is a reserve officer, plays a role in a civic association, and in addition has a social life that brings him into contact with diverse social strata.<sup>3</sup>

The Internet once looked like the perfect realization of Simmel’s vision of freely developing multifaceted selves. In the beginning, the Internet made it easy for the like-minded, no matter what the “like,” to meet with whatever degree of disclosure they desired. The days are gone when no one knew you were a dog.<sup>4</sup> Advances in information processing technology give *others* considerable power to collect, analyze, and distribute one’s information, often personally identifying one in the process.<sup>5</sup> We focus on a single consequence: the impact on the self.<sup>6</sup>

---

Michael Froomkin, *The Death of Privacy*, 52 STANFORD LAW REV. 1461, 1462 (2000) (“I will use ‘informational privacy’ as shorthand for the ability to control the acquisition or release of information about oneself”); *Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 763 (1989) (“both the common law and the literal understandings of privacy encompass the individual’s control of information concerning his or her person”).

<sup>2</sup> Felix Strouhal, *PRIVACY IN SMALL TOWNS? NON-EXISTENT* (2010), [www.bridge-online.cz/get.php?id=586](http://www.bridge-online.cz/get.php?id=586).

<sup>3</sup> Quoted in JERRY Z. MULLER, *THE MIND AND THE MARKET: CAPITALISM IN WESTERN THOUGHT* 248 – 249 (2003).

<sup>4</sup> “On the Internet no one knows that you are a dog” is the caption to Peter Steiner’s iconic 1993 New Yorker cartoon that captured the spirit of the Internet at the time. Peter Steiner, *On the Internet, no one knows your a dog*, 69 THE NEW YORKER, 1993, at 61.

<sup>5</sup> See, e.g., COMMENTS OF THE CENTER FOR DIGITAL DEMOCRACY AND U.S. PIRG, IN THE MATTER OF A PRELIMINARY FTC STAFF REPORT ON PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 15–20 (2011), <http://www.ftc.gov/os/comments/privacyreportframework/00338-57839.pdf>.

We limit our discussion to the private sector, but this is not to ignore governmental surveillance. “The primary business model of the Internet is built on mass surveillance, and our government's intelligence-gathering agencies have become addicted to that data. . . The result is a corporate-government surveillance partnership, one that allows both the government and corporations to get away with things they couldn't otherwise.”<sup>7</sup> Constraining private data collection is one piece of the solution to constraining the government's use of data. We further limit our private sector discussion to businesses and do not address the important fact that individuals can, and do, easily find out an immense amount of information about each other. This also can have a profound impact on how you act, as illustrated by one commentator's question,

What do you do before a first date? . . . [Y]ou may be forgetting the most critical one, the big G . . . I am suggesting that you spend some time sprucing up your online image (with as much if not more intensity as your physical image) before truly opening up and letting someone into your world . . . Google gives people the power to get to know you without ever actually having to meet you. It's best to just treat your personal online brand as though you're going on countless first dates.<sup>8</sup>

Our concern is precisely that people may come to think of their words and actions as contributing to a publicly accessible “brand” that they must keep “spruced up,” and while we limit our discussion to businesses, much of what we say also applies to individuals.

---

<sup>6</sup> The connection between privacy and the self is a standard theme in the privacy literature. *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008) (“Theorists have proclaimed the value of privacy to be protecting intimacy, friendship, individuality, human relationships, autonomy, freedom, self-development, creativity, independence, imagination, counterculture, eccentricity, thought, democracy, reputation, and psychological well-being”). The NSA's surveillance activities have sparked concern about the self. *See* Michael P. Lynch, PRIVACY AND THE THREAT TO THE SELF THE NEW YORK TIMES, OPINONATOR (2013), <http://mobile.nytimes.com/blogs/opinionator/2013/06/22/privacy-and-the-threat-to-the-self> (“To the extent we risk the loss of privacy we risk, in a very real sense, the loss of our very status as subjective, autonomous persons”).

<sup>7</sup> Bruce Schneier, THE PUBLIC-PRIVATE SURVEILLANCE PARTNERSHIP, SCHNEIER ON SECURITY (2013), <https://www.schneier.com/essay-436.html>. For an illuminating analysis of the modern relation between democracy and corporate power, see SHELDON SANFORD WOLIN, DEMOCRACY INCORPORATED: MANAGED DEMOCRACY AND THE SPECTER OF INVERTED TOTALITARIANISM (2010).

<sup>8</sup> Slyvia Dziedzic, HOW TO LOSE A DATE IN 10 SEARCH RESULTS (LOOKING GOOD ONLINE FOR A FIRST DATE), BRAND YOURSELF (2011), <http://blog.brandyourself.com/product-tutorials/how-to-lose-a-date-in-10-search-results/>.

Section I presents the realization of a multifaceted self as an essential ideal and argues that such selves are realized through social roles that mediate interactions with others. The successful realization of a multifaceted self requires privacy in public, a concept the section characterizes. Section II argues that informational norms play a central role in the creation of privacy in public. Section III provides essential analytical tools by giving an explicit account of norms. Sections IV and V use those tools to explain how the rise of the Internet and rapid advances in information processing technology undermine norm-created privacy in public is crumbling and along with it the privacy in public essential to the realization of a multifaceted self. Restoring privacy in public requires restoring and creating appropriate informational norms. Sections VI and VII considers the prospects for doing so.

In foregoing summary, legal regulation is noteworthy by its absence. Our results are nonetheless highly relevant to privacy regulation. A critical task for such regulation, as well as public policy generally, is the creation of appropriate informational norms. One of our primary motives is to reorient privacy regulation toward that task.

## I. THE SELF AND SOCIAL ROLES

We make three claims. First, the realization of a multifaceted self is an ideal which you strive to realize. Second, you realize such a self in large part through social roles that mediate interactions with others. Third, today such realization requires a significant degree of “privacy in public.” The appeal to “privacy *in public*” may look like the wilful embrace of a contradiction.<sup>9</sup>

---

<sup>9</sup> Helen Nissenbaum was, as far as we know, the first to explicitly recognize the importance of privacy in public for the analysis of legal and policy issues surrounding privacy. See Helen Nissenbaum, *Toward an Approach to Privacy in Public: The Challenges of Information Technology*, 7 ETHICS BEHAV. 207 (1997), and Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in*

Private and public are opposites, after all: “purely ‘private’ things are completely inaccessible to others. Purely ‘public’ [things] are completely accessible to others.”<sup>10</sup> We begin with an explanation of privacy in public, and then argue for each of our claims in turn.

#### A. The Concept of Privacy in Public

Opposition need not mean contradiction; rather, “[p]rivacy and publicity . . . are each defined with and by each other along [a] conceptual sliding scale.”<sup>11</sup> Your degree of informational privacy—your place on the scale—is a function of how much you can control what others do with information about you. You can have control *in public*. A closer the privacy cities offer shows how. Cities offer *privacy by obscurity* and *privacy by voluntary restraint*. Privacy by obscurity is essentially a matter of getting lost in the crowd, something a city’s physical size and large population makes relatively easy. As E. B. White famously observed, cities “bestow the gift of loneliness and the gift of privacy.”<sup>12</sup> Simmel likewise extolls privacy by obscurity, but he also emphasizes privacy by voluntary restraint. He was impressed by the fact that people voluntarily limit their knowledge of each other as they interact in a wide variety of social roles. Merchants and customers, students and teachers, restaurant customers and waiters, for example,

---

*Public*, 17 LAW PHILOS. 559–596 (1998). These articles introduced us to the concept of privacy in public, and our approach in terms of norms is also deeply indebted to her work. For later recognitions of privacy in public, see James H. Patton, *Protecting privacy in public? Surveillance technologies and the value of public places*, 2 ETHICS INF. TECHNOL. 181 (2000); Herman T. Tavani, *Search Engines, Personal Information and the Problem of Privacy in Public*, 3 INT. REV. INF. ETHICS (2005), [http://www.i-r-i-e.net/inhalt/003/003\\_tavani.pdf](http://www.i-r-i-e.net/inhalt/003/003_tavani.pdf); and Nick Taylor, *State Surveillance and the Right to Privacy*, 1 SURVEILL. SOC. (2002), <http://www.surveillance-and-society.org/articles1/statesurv.pdf>. A 2013 report from Canada’s Information and Privacy Commissioner emphasizes the importance of privacy in public. ANN CAVOUKIAN, SURVEILLANCE, THEN AND NOW: SECURING PRIVACY IN PUBLIC SPACES (2013), <http://www.ipc.on.ca/images/Resources/pbd-surveillance.pdf>. There is a well-established practice in sociology of regarding privacy as existing in public through selective disclosure. See, e.g., CHRISTENA E. NIPPERT-ENG, ISLANDS OF PRIVACY (2010).

<sup>10</sup> NIPPERT-ENG, *supra* note 9 at 4.

<sup>11</sup> *Id.* at 4.

<sup>12</sup> E. B. WHITE, HERE IS NEW YORK 1 (1999).

typically exchange only the information necessary to their interaction in those roles and voluntarily refrain from requesting, disclosing, or otherwise discovering more.<sup>13</sup>

Advances in information processing are eroding privacy in public. This is plain for privacy by obscurity. A variety of technologies make it increasingly hard to hide: video surveillance,<sup>14</sup> facial recognition software,<sup>15</sup> license plate readers,<sup>16</sup> and communications monitoring,<sup>17</sup> for example. As privacy by obscurity declines, the need for privacy by voluntary restraint increases, and we focus on the latter in part for that reason, and in part because the loss of privacy by obscurity is well-studied already and the erosion of privacy by voluntary restraint has received far less attention. Unfortunately, technology-driven business practices have already so greatly reduced privacy by voluntary restraint that

we no longer move about our lives as self-contained beings, but as nodes of information production in a dense network of digital relations involving other nodes of information production. All of the data about us as individuals in social network communities is

---

<sup>13</sup> Georg Simmel, *The Sociology of Secrecy and Secret Societies*, 11 AM. J. SOCIOL. 441, 468 (1906).

<sup>14</sup> BILGE YESIL, VIDEO SURVEILLANCE POWER AND PRIVACY IN EVERYDAY LIFE (2009) Some recent developments are striking. Consider LED-based streetlights with a Wi-Fi connection, broadcast speaker, audio and video recorders, proximity sensors, and video displays (<http://intellistreets.com>).

<sup>15</sup> See, e.g., Chicago police start using facial-recognition software to arrest suspects, <http://rt.com/usa/chicago-police-cctv-surveillance-135/> (last visited Feb 9, 2014); and Next Generation Identification, FBI, [http://www.fbi.gov/about-us/cjis/fingerprints\\_biometrics/ngi/ngi2](http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/ngi2) (last visited Feb 9, 2014).

<sup>16</sup> Vehicle Inspection System, PERCEPTICS: IMAGING TECHNOLOGY SOLUTIONS (2014), <http://www.perceptics.com/products/uvis-ig-uvis-sm/vehicle-inspection-system-vis-software.html> (“When security and operating efficiency demand the most robust, easy to use imaging systems, you need the Vehicle Inspection System (VIS) software. VIS is Perceptics’ proprietary visual database, which integrates high-resolution images captured by our License Plate Reader, Under Vehicle Inspection Systems, DriverCam and SceneCam devices into a searchable database. VIS seamlessly ties into back-end databases so you can capture data, check white lists and make informed decisions.”).

<sup>17</sup> Consider the database technology from Palantir. Palantir, PALANTIR TECHNOLOGIES, <https://www.palantir.com/> (last visited Feb 9, 2014). It ties “together surveillance video outside a drugstore with credit-card transactions, cell-phone call records, e-mails, airplane travel records, and Web search information.” Ashlee Vance & Brad Stone, *Palantir, the War on Terror’s Secret Weapon*, BUSINESSWEEK: MAGAZINE, 2011, <http://www.businessweek.com/magazine/palantir-the-vanguard-of-cyberterror-security-11222011.html> (last visited Feb 9, 2014). Database searches can be combined with predictive analytics to (attempt to) identify threats before they occur. See, e.g., What is Web Intelligence?, RECORDED FUTURE, <https://www.recordedfuture.com/web-intelligence/> (last visited Feb 9, 2014).

owned, operated, managed, and manipulated by third parties beyond our control, and those third parties are, typically, private companies.<sup>18</sup>

We explain how to reclaim privacy in public. Our solution appeals to informational norms, social norms that constrain the collection, use, and distribution of personal information.<sup>19</sup> The constraints facilitate the voluntary restraint essential to privacy in public. For convenience, we will from now on mean by “privacy in public” privacy in public *by voluntary restraint*, except where we indicate otherwise.

### B. The Ideal of a Multifaceted Self

William James offers a useful initial characterization of the relevant notion of the self. “I am,” James writes,

often confronted by the necessity of standing by one of my . . . selves and relinquishing the rest. Not that I would not, if I could, be both handsome and fat and well dressed, and a great athlete, and make a million a year, be a wit, a *bon vivant*, and a lady killer, as well as a philosopher, and a philanthropist, statesman, warrior, and African explorer, as well as a ‘tone poet’ and saint. But the thing is simply impossible . . . Such characters may at the outset of life be alike *possible* to a man. But to make anyone of them actual, the rest must be more or less suppressed. So the seeker of his truest, strongest, deepest self must review the list carefully, and pick out the one on which to stake his salvation.<sup>20</sup>

---

<sup>18</sup> RONALD J DEIBERT, BLACK CODE: INSIDE THE BATTLE FOR CYBERSPACE \_\_\_\_ (2011).

<sup>19</sup> Simmel’s explanation of privacy in public appeals to directly to the self (“personality” in Simmel’s terminology). To see how, recall Simmel’s observation that, in certain relationships, “we have to do with a quite typical boundary, . . . with reference to which . . . the outside party, in observance of conventional discretion, does obtrude by questions or otherwise.” Simmel, *supra* note 13 at 454. “Discretion,” he continues, “is nothing other the sense of justice with respect to the sphere of the intimate contents of life.” *Id.* at 454. The “radius of that sphere . . . marks out the distance which a stranger may not cross without infringing on another’s honor.” *Id.* at 453. Simmel explains that to “penetrate this circuit by curiosity is a violation of his personality.” *Id.* The boundary is really myriad different boundaries defined by different shared conceptions of role-appropriateness. People respect these boundaries, not (or at least not primarily) to avoid “infringing another’s honor,” but because they adhere to the relevant norms.

<sup>20</sup> WILLIAM JAMES, 1 THE PRINCIPLES OF PSYCHOLOGY 309 (1890).

The essential point is that you make yourself who you are by what you “stand by,” by the commitments you strive to realize.<sup>21</sup> One emendation is required.

James contends (at least in this passage<sup>22</sup>) that *one* central commitment defines who you are, but selves consist of multiple commitments. As John Gray notes,

We are none of us defined by membership in a single community or form of moral life. We are . . . heirs of many distinct, sometimes conflicting, intellectual and moral traditions. . . . The complexity and contradictions of our cultural inheritance give to our identities an aspect of complexity and even of plurality which is . . . essential to them. . . . [T]he power to conceive of ourselves in different ways, to harbour dissonant projects and perspectives, to inform our thoughts and lives with divergent categories and concepts, is integral to our identity as reflective beings.<sup>23</sup>

The self you seek to realize is a multifaceted self. This conception underlies liberal political philosophy.<sup>24</sup> We place ourselves in this tradition, and assume that the realization of a multifaceted self is an ideal people strive to realize.

### C. Social Roles

It is common to complain that liberal political philosophy assumes that “selfhood . . . is transcendent and immaterial”<sup>25</sup> and that “one’s self has a nature that is independent of any social

---

<sup>21</sup> There is more than one candidate for the label “concept of the self.” In particular, there are “pure ego” or “center” theories. See C. D BROAD, *THE MIND AND ITS PLACE IN NATURE* 558f. (2009), and COLIN MCGINN, *THE CHARACTER OF MIND: AN INTRODUCTION TO THE PHILOSOPHY OF MIND* 111f. (2 ed. 1997). For a commitment based theory of the self, see RICHARD WARNER, *FREEDOM, ENJOYMENT, AND HAPPINESS: AN ESSAY ON MORAL PSYCHOLOGY* (1987).

<sup>22</sup> It is not at all clear that James actually thought you had to single out one self. As he notes elsewhere, “Properly speaking, a man has as many social selves as there are individuals who recognize him and carry an image of him in their mind . . . Nothing is commoner than to hear people discriminate between their different selves of this sort: ‘As a man I pity you, but as an official I must show you no mercy; as a politician I regard him as an ally, but as a moralist I loathe him;’ etc., etc.” JAMES, *supra* note 20 at 295.

<sup>23</sup> JOHN GRAY, *POST-LIBERALISM: STUDIES IN POLITICAL THOUGHT* 262 – 263 (1993).

<sup>24</sup> JOSEPH RAZ, *THE MORALITY OF FREEDOM* (1986). For an excellent overview, see John Christman, *Autonomy in Moral and Political Philosophy*, in *THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY* (Edward N. Zalta ed., Spring 2011 ed. 2011), <http://plato.stanford.edu/archives/spr2011/entries/autonomy-moral/> (last visited Feb 16, 2014).

context one may seek its realization.”<sup>26</sup> We neither assert nor deny that the self has a transcendent nature independent of social contexts. We need only the uncontroversial claim that the roles through which you define yourself are, by and large, social roles, roles provided by the society—or perhaps better, the societies—in which you live.<sup>27</sup>

You could not, for example, be a bird-watcher in a society that does not recognize that role. Try to imagine the opposite. Imagine a primitive tribe whose sole use for animals is to hunt and eat them; you are the lone anomaly who tracks birds merely to look at them.<sup>28</sup> Although you watch birds, you are not a bird watcher in the sense that a member of the Audubon Society is. To call yourself a bird watcher in that sense is to ascribe to yourself a *recognized role*.

Contemporary society not only recognizes that people may enjoy bird-watching, it recognizes that behavior pattern as an avocation, not as deviant and bizarre. In the primitive tribe, you cannot refer to an accepted social role to explain your bird gazing to yourself and others. You are just deviant. Similarly, you cannot be a lawyer except in a society governed by law; practice medicine unless society recognizes the practice; be a professional race car driver except in a community that recognizes the sport.<sup>29</sup> Even being a parent, child, lover, or spouse takes on different meanings and definitions depending on the society in which the relationship is realized.

To avoid misunderstanding, we should emphasize that we are not saying that one’s possibilities or self-realization are *completely* circumscribed by the social roles one’s society

---

<sup>25</sup> JULIE E. COHEN, *CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE* 16 (2012). We take Cohen to be reacting to “pure ego” theories mentioned in Note 21.

<sup>26</sup> *Id.* at 16. For a response, see, e.g., WILL KYMLICKA, *LIBERALISM, COMMUNITY, AND CULTURE* (1989).

<sup>27</sup> RAZ, *supra* note 24 at 311 (emphasizing the importance of social roles—what he calls “social forms”—to the development of the self).

<sup>28</sup> The example is from *Id.* at 310.

<sup>29</sup> See *Id.* at 310.

offers. There are clear examples to the contrary.<sup>30</sup> Such examples do not, however, undermine our point that for the most part the roles through which one realizes a multifaceted self are social roles recognized in the society in which one lives.

#### D. The Need for Privacy in Public

Realizing multiple social roles requires a significant degree of privacy in public.<sup>31</sup>

Disapproval and its consequences are perhaps the most obvious reason. Some think that it is wrong to combine being gay or lesbian with being a parent and seek to prevent it. Exploring sexuality in sex clubs is, in the eyes of many, unacceptable in a candidate for political office.<sup>32</sup> Many parents would have qualms about an exemplary elementary school teacher who at night drinks himself or herself into oblivion while indulging a passion for (legal) pornography. An associate in a traditional, conservative law firm might face strong disapproval and even

---

<sup>30</sup> Suppose that you live in a yet to be discovered primitive tribe, isolated from the rest of the world. The men buy and sell their wives, and women are generally regarded as fungible property. You are the sole voice for gender equality. While the tribe recognizes other applications of the concept of equality, gender equality seems ludicrous at best, unintelligible at worst. So, as with the anomalous bird-watcher, neither you nor your society can understand your gender equality claims with reference to a *recognized social role*, at least not the role of “advocate for gender equality.” *You*, however, can still understand yourself as committed to gender equality and that commitment can play a central role in your self-definition. You are just extending your society’s notion of equality into a new area. The bird watcher example may be different because it may be harder for the bird watcher to find a ready basis for extension in existing notions of watching and observing.

<sup>31</sup> “Because our ability to control who has access to us, and who knows what about us, allows us to maintain the variety of relationships with other people that we want to have, it is, I think, one of the most important reasons why we value privacy.” James Rachels, *Why Privacy Is Important*, 4 *PHILOS. PUBLIC AFF.* 323, 329 (1975).

<sup>32</sup> See Sarah Hall, *JERI RYAN SEX-CLUB SCANDAL* (2004), <http://www.movies.eonline.com/News/Items/0,1,14366,00htm>. Jack Ryan’s desire to explore sex with his famous actress wife Jeri Ryan in a sex club may have been responsible for President Obama’s election to the US Senate in 2004. Ryan had won the Republican primary for that Senate race and appeared to have a reasonable chance of defeating Obama in the general election—until the news about the sex club broke. Ryan was forced to withdraw from the race, and the Republican party of Illinois selected the relatively unknown Alan Keys to replace Ryan. By Dan Collins AP June 25, 2004 & 7:42 Am, *SEX SCANDAL ENDS RYAN SENATE BID*, <http://www.cbsnews.com/news/sex-scandal-ends-ryan-senate-bid/> (last visited Feb 15, 2014). Obama went on to win the general election in a landslide. See *WP Politics*, November 24, 2004.

termination of employment if the senior partners discovered the associate's anonymous calls for radical reform of the legal profession. A thirty-five-year-old man who has lived a law-abiding and exemplary life as a pediatrician, husband, and parent may face family turmoil and employment problems when the hospital in which he works and his family learn of his arrest for possessing an ounce of marijuana at nineteen and his violation of sodomy laws in his one homosexual relationship at twenty-two. In general, the expectations we create in others when we are in one role may be deeply disappointed when they find us in what they regard as an incompatible role. The consequences range from disapproval to ostracism. Disapproval and reprisal are, however, not the only—nor even perhaps the most important—reasons the realization of a multifaceted self requires privacy in public. Realizing such a self also requires that others not know certain things even if their knowing them would have no adverse consequences. To see why, consider two examples.

For the first, imagine you eat once or twice a week in a small Italian bistro. The waiters and the owner engage you in brief casual conversation, and you want the interaction to stop there. You go to the restaurant for a pleasant break from the rest of your life, for an experience as disconnected as possible from that life. You do not want them to know, for example, that you are the CEO of an international business. Your concern is not just that the knowledge could change the way they relate to you and open the door to further questions; you do not want to have even to *think* about whether it *might* do that. You want to play the role of “customer they know very little about.” You cannot do that if they know too much about you. It does not matter if they approve, disapprove, or are indifferent. All that matters is what they know.<sup>33</sup> This is just one

---

<sup>33</sup> Students of Foucault will point out that the “most sinister thing about surveillance is that, merely to observe and assess, it must establish standards, which is to say it must arbitrarily assign values of normalcy to some aspects of human conduct in order to gauge the deviation of others. Watching means prescribing. As the process extends into each facet of life, everything becomes the object of a totalizing

instance of the general fact that how a person appears to others depends on what those others know; a person cannot, for example, appear truthful to those who know the person is a liar. The example also illustrates another important general truth: a person cannot control the way he or she appears entirely through his or her own efforts. In the restaurant, for example, you need the waiters' and owner's cooperation. They must refrain from finding out about you by asking probing questions you answer to avoid an uncomfortable situation; looking through the wallet you inadvertently left behind; using Google, Spokeo, or Lexis/Nexis; hiring private detectives; or, following you around themselves.

The second example is the student/teacher relationship. Teachers, teachers at large universities in particular, typically have more or less limited knowledge about their students. The limited knowledge has important consequences for the way students appear to teachers. They appear primarily in the light of their relevant academic achievements, not in light of extracurricular aspects of their personalities, past academic records, honors conferred or punishments endured. This helps ensure that students are evaluated only on the basis of relevant academic work. Students similarly have limited knowledge of teachers. Not only does it help ensure that students evaluate them primarily in terms of their educational effectiveness, it also allows teachers to model an intellectual or professional style in an approach to a topic that students can adopt and adapt precisely because it is not tightly tied to a personal style and history. Students and teachers need

---

'gaze,' a kind of visual tractor beam that bends people to its standards just by looking at them." Ariel Ron, *AMERICAN PANOPTICON: HOW A SMALL TOWN FORESHADOWED THE SURVEILLANCE STATE, THE APPENDIX* (2013), <http://theappendix.net/blog/2013/11/american-panopticon>. We do not dispute the claim. Our point is that merely knowing also has consequences. Sartre makes this point. JEAN PAUL SARTRE, *BEING AND NOTHINGNESS*. 344 (1984) ("If the Other-as-object is defined in connection with the world as the object that sees what I see, then my fundamental connection with the Other-as-subject must be able to be referred back to my permanent possibility of being seen by the Other."). James Patton quotes this passage from Sartre in support of his claim that "surveillance . . . changes the experience of being in a place." Patton, *supra* note 9 at 184.

each other's cooperation to maintain these limits on what they know; they must voluntarily refrain from finding out too much about each other.

Similar remarks hold for a wide variety of social roles. Acquaintances, colleagues, friends, and family, for example, typically can acquire different ranges of information. Further, different buyer/seller relationships allow and disallow different inquires. Pharmacists can ask what other drugs you are taking to guard against drug interactions, but not about whether you are happy in your personal relationships; your internist can ask about both.<sup>34</sup> A washing machine salesperson can ask how frequently you plan to do laundry, but not whether you text or email more, whereas the opposite is true for an Apple store salesperson.

In general, selective disclosure is a characteristic of our relationships with others.

As the sociologist Nippert-Eng emphasizes:

At its core, managing privacy is about managing relationships between the self and others. . . . privacy . . . [is] a "boundary regulatory process by which a person (or group) makes himself more or less accessible and open to others." When we regulate our accessibility to others—including the accessibility of information, objects, space, time, or anything else that we deem private—we simultaneously regulate our relationships with them.<sup>35</sup>

She notes that "secrecy is the condition in (and through) which we try to insist that our private things are as private as we wish them to be. Secrecy is a means to an end, a process in which we actively work to manage our private matters."<sup>36</sup> She explains that

No matter what the secret, no matter how it is manipulated or what its fate, to consider a secret is to simultaneously consider the relationships (perhaps entire social networks) that it throws into relief. Indeed, from a sociological perspective, perhaps the most significant aspect of secrets is their selectively shared nature. They are secrets with and secrets from, intentionally disclosed to and concealed from specific individuals at specific times and in

---

<sup>34</sup> At least under some circumstances since your internist has a professional duty to monitor your mental health to some extent.

<sup>35</sup> NIPPERT-ENG, *supra* note 9 at 22.

<sup>36</sup> *Id.* at 24.

specific ways. Simultaneously inclusive and exclusive, secrets are quite effective at achieving social boundary work, an excellent measure of the social distance between individuals.<sup>37</sup>

While we emphasize the place of social roles in determining selective disclosure, Nippert-Eng takes a much broader view. She is concerned with “the daily activity of trying to deny or grant varying amounts of access to our private matters to specific people in specific ways,”<sup>38</sup> and social roles are just one aspect of the activity. Nippert-Eng nonetheless provides ample illustration of the place of roles in creating privacy in public.<sup>39</sup>

## II. INFORMATIONAL NORMS AND THE CREATION OF PRIVACY IN PUBLIC

People achieve selective disclosure through interaction in a variety of social roles. It is an astonishing feat of coordination. How do restaurants, students, teachers, friends, pharmacists, software sellers, and so on—and indeed *on and on*—know what the permissible informational boundaries are? And, how does the coordination happen effortlessly, without thought or explicit negotiation? Through informational norms.

### A. Informational Norms

As Helen Nissenbaum notes, informational norms

circumscribe the type or nature of information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed. In medical contexts, it is appropriate to share details of our physical condition or, more specifically, the patient shares information about his or her physical condition with the physician but not vice versa; among friends we may pour over romantic entanglements (our own and those of others); to the bank or our creditors, we reveal financial information; with our

---

<sup>37</sup> *Id.* at 27.

<sup>38</sup> *Id.* at 2.

<sup>39</sup> *See, e.g., Id.* at chapter 2.

professors, we discuss our own grades; at work, it is appropriate to discuss work-related goals and the details and quality of performance.<sup>40</sup>

Informational norms constrain the collection, use, and distribution of information. The constraints vary as the relevant social roles vary. Accordingly, we focus on informational norms that take this general form: people shall collect, use, and distribute information only in ways appropriate to their respective social roles.<sup>41</sup> We will refer to these as *role-appropriate* informational norms.<sup>42</sup> It is convenient to give “collection,” “use,” and “distribution” more precise and restricted meanings than they normally carry. It is convenient to define “use” first. By “use” we mean taking affirmative action to allocate different costs and benefits to different individual based on information about them—setting health care premiums and determining whom to hire, for example. By “collection,” we mean the acquisition of information that results in *merely knowing* (or having an opinion) about people without (yet) taking affirmative steps to allocate costs

---

<sup>40</sup> Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. LAW REV. 119, 120–121 (2004). See also HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* (2010); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DEDALUS 32 (2011).

<sup>41</sup> We formulate informational norms differently in ROBERT H. SLOAN & RICHARD WARNER, *UNAUTHORIZED ACCESS: THE CRISIS IN ONLINE PRIVACY AND INFORMATION SECURITY* (2013). In mass market seller/consumer contexts, we take them to be of the following form: buyers demand that the seller collect, use, and distribute information only as is appropriate for that seller’s role. We use “demand” in the economist sense of “willing to pay for.” On this treatment, sellers are not parties to the norm. Instead, mass market norms unify buyers’ demands. We argue that, under conditions that adequately approximate perfect competition, sellers will conform to norms because that will be the profit maximizing strategy. For detailed analysis of the role of norms in markets, we prefer the foregoing “consumers only” formulation of informational norms, but the formulation in the text (which treats businesses as well as buyers as parties to the norm) is more intuitive and adequate for our purposes here.

<sup>42</sup> We introduced the term “role appropriate” in *Id.*, where we discuss the concept at length. “Role appropriateness” is determined contextually. Over a wide range of cases, group members share a complex of values that leads them to more or less agree in their particular contextual judgments of appropriateness. “Within each context, the relevant agents, types of information, and transmissions principles combine to shape the governing informational norms.” Michael Zimmer, *Privacy on Planet Google: Using the Theory of “Contextual Integrity” to Clarify the Privacy Threats of Google’s Quest for the Perfect Search Engine*, 3 J BUS TECH L 109, 115 (2008). Norms vary from group to group. For simplicity, however, we take the relevant group to be all United States consumers.

and benefits. We understand “distribution” to be the further dissemination of previously collected data.

The examples that follow illustrate the way in which role-appropriate informational norms create privacy in public. We illustrate collection, use, and distribution separately, but each example if fully described would exhibit all three. For the sake of contrast later, we describe the examples against a mid-twentieth century background. In the 1950s, data collection was in its infancy, with only the beginnings of credit reporting practices.<sup>43</sup> Direct marketing was not widely used until the 1970s.<sup>44</sup> People did of course disclose information to businesses, governmental and private licensing agencies, and so on, but the information was typically stored in geographically scattered paper records, and there was no convenient way to search all of it. As a result, in the 1950s people still retained significant control over their information.

#### B. Collection: Constraints on Merely Knowing

Return to the restaurant example. You have an interest in sharing information in ways that meet your needs, and the restaurant would like to meet those needs since it wants your repeat business. How do you and the restaurant coordinate to realize this shared interest?

Through a role-appropriate informational norm. Within limits, it is role appropriate for the restaurant to collect (and use and distribute) customers’ personal

---

<sup>43</sup> See RULE, *supra* note 1 at Chapter III (discussing the history of credit reporting).

<sup>44</sup> See DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 18 (2004). Prior to 1970, was difficult to differentiate among consumers. In 1970, the change came when the government began selling census data on magnetic tapes.

information in ways that meet the customers' restaurant needs.<sup>45</sup> The boundaries of “within limits” and “restaurant needs” are quite indeterminate, but, until relatively recently, that did not matter much since the customers were the main source of the restaurant's information about them, and they could draw the boundaries the way they wanted.<sup>46</sup> Customers and restaurants could coordinate on information processing without explicit negotiation—indeed, with hardly a thought about it. The restaurant could ask the number people in a party, provide a menu (in some form), offer non-menu information about the food, and so on; on the other hand, it would refrain from more pointed inquiries unless, and only to the extent that, the customer opened the door to such questions (for example, by answering the pro forma, “How are you tonight?” with, “Just back from Europe. Have you been there?”). The result was privacy in public: norm-created selective disclosure that secured the benefits of information processing to the extent that it allowed it, and that protected privacy to the extent it did not.

Similar remarks hold for the student-teacher relationship and a wide range of other interactions through social roles. Informational norms facilitated the coordination essential to privacy in public. The indeterminate boundaries did not matter because individuals retained considerable control over information about them and so could in indeterminate areas disclose or conceal as they wished.

---

<sup>45</sup> See John Mariani, WHAT YOUR FAVORITE RESTAURANTS KNOW ABOUT YOU, *EAT LIKE A MAN* (2011), <http://www.esquire.com/blogs/food-for-men/great-restaurant-service-110811>.

<sup>46</sup> See Chris Schonberger, THE 20 MOST ANNOYING THINGS SERVERS DO AT RESTAURANTS: OVERSHARE ABOUT THEIR DAY, THEIR JOB, OR THEIR LIFE BEYOND THE RESTAURANT, *FIRST WE FEAST* (2013), <http://firstwefeast.com/laugh/the-20-most-annoying-things-servers-do-at-restaurants/s/overshare-about-their-day-their-job-or-their-life-beyond-the-restaurant/> (“Restaurants are awkward. But we also all know how to play this game, so don't break the fourth wall and talk about how you are actually a marine biologist and you're getting ready to move to Alaska to study whales—or, worse still, tell a sob story about how another table stiffed you on a tip. Keep it professional, and we promise to not drag you into our arguments and ask you to arbitrate. The less we know about each other, the better.”).

Collection is a case of “merely knowing” (as we are using the term), and the concern is that what others know about you affects the way you can appear to them. Controlling what others know is, however, not the only way to control how you appear. You can control *yourself*. You will not run the risk of appearing as a lawyer who advocates radical judicial reform, or as a politician that goes to sex clubs if you do not call for reform or frequent sex clubs. The *use* of information—in our sense of “use to allocate costs and benefits”—can create incentives for one to control what one does and says.

### C. Use: The Allocation of Risks and Benefits

In market economies, private businesses play a significant role in the distribution of costs and benefits across society. The distribution is a function of the employment opportunities the businesses provide and the price and type of goods and services they offer. Businesses allocate employment based on the way people appear to them, and the same is true of goods and services (different types of consumers may receive different advertising and different prices<sup>47</sup>). You can maximize the extent to which the watchers will view your profile with favorable eyes by controlling what you do, with whom you associate, and what you say.

Employment applications are a good example. Employers and applicants have both overlapping and opposing interests. Employers want the information that will best enable them to determine if the applicant is a good fit for the job. Applicants too have an interest in a good fit, but also have an incentive to withhold unfavorable information as well as to limit even favorable or neutral information to keep aspects of their lives private from a potential employer. A role-appropriate informational norm coordinates the information exchange. It is role-appropriate for

---

<sup>47</sup> See *infra* note 57 (discussing price discrimination).

employers to collect a relevant range of information regarding the suitability of applicants for employment and use that information in employment decisions.

The references to “a relevant range” and “suitability” introduce considerable indeterminateness into what the norm prohibits. This is not to deny that there are clear cases. No one would object to providing references from past employers, providing a resume, and being interviewed, and, where relevant, providing certifications of expertise. In addition, state and federal law prohibit a wide range of inquiries, including inquires about race, sex, national origin, religion, age, or disability, and whether the applicant has children.<sup>48</sup> The restrictions are easy to circumvent, however. Employers can simply ask questions that allow them to infer what they cannot ask directly—for example, “When did you graduate from high school or from college?” as a way to infer age,<sup>49</sup> and, as long as it is arguably job related, “What is your experience with such-and-such age group?” as a way to discover if the applicant has children.<sup>50</sup> In addition, employers can ask job applicants to waive privacy rights.<sup>51</sup> The upshot is that employers have considerable latitude in determining what they will regard as information relevant to suitability for employment.

As in the restaurant example, this indeterminateness did not matter greatly as long as limited access to data and limited information processing abilities gave applicants considerable

---

<sup>48</sup> See PRIVACY IN EMPLOYMENT LAW, Fourth Edition, BLOOMBERG BNA 230 – 325, <http://www.bna.com/privacy-employment-law-p17179869438/> (last visited Feb 8, 2014).

<sup>49</sup> See Alison Doyle, AGE-RELATED INTERVIEW QUESTIONS EMPLOYERS SHOULDN'T ASK, ABOUT.COM, <http://jobsearch.about.com/od/how-to/fl/age-related-interview-questions.htm>.

<sup>50</sup> See Interview Questions You Can't Ask and Legal Alternatives, KETTERING UNIVERSITY, [https://kettering.edu/sites/default/files/resource-file-download/Interview%20Questions%20Not%20to%20Ask\\_1.pdf](https://kettering.edu/sites/default/files/resource-file-download/Interview%20Questions%20Not%20to%20Ask_1.pdf).

<sup>51</sup> There are limits. Applicants can consent to credit checks under federal law, but state law may prohibit checks even with employee consent. Use of Credit Information in Employment 2011 Legislation, December 19, 2011, NATIONAL CONFERENCE OF STATE LEGISLATURES (2011), <http://www.ncsl.org/research/financial-services-and-commerce/use-of-credit-information-in-employment-2011-legis.aspx>.

control over what employers could discover about them.<sup>52</sup> A norm-implemented tradeoff was again the result. Employers were assured a range of relevant information, but norm-imposed boundaries ensured that they could not reach too far into applicants' personal lives. The selective disclosure of privacy in public was again the result. There are many examples, such as: health insurance,<sup>53</sup> direct marketing,<sup>54</sup> the extension of credit,<sup>55</sup> news reporting,<sup>56</sup> and the practice of price discrimination.<sup>57</sup> These differ importantly among themselves, but it is the common pattern of selective constraint though role-appropriate norms that concerns us.

#### D. Distribution: The Multiplier

Distribution multiplies the effects of collecting and using data. To see how, think of the type of information flow collection and use create. It is a simple hub-and-spoke structure. The hub is a person, and each spoke leads to an entity that collects and possibly uses information about the person. Distribution complicates this structure. An entity at the end of a spoke can distribute information to any number of other entities, which may distribute the information to any number of entities, and so on. The simple hub-and-spoke structure becomes a web of

---

<sup>52</sup> The problem was to constrain employers' overbroad interpretation of the norm by asking indirect questions. But well prepared applicants could do so. This is what one should expect with partly overlapping, party opposed interests—a give and take in which standards develop.

<sup>53</sup> See SLOAN AND WARNER, *supra* note 41 at 107 - 109.

<sup>54</sup> See RULE, *supra* note 1 at 104; SLOAN AND WARNER, *supra* note 41 at 96 - 103; DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 18 (2004).

<sup>55</sup> See Priscilla M. Regan, *The United States*, in JAMES B RULE & GREENLEAF, *GLOBAL PRIVACY PROTECTION: THE FIRST GENERATION* 50 (2010).

<sup>56</sup> See JON L. MILLS, *PRIVACY: THE LOST RIGHT* 287 (2008).

<sup>57</sup> Price discrimination is charging different buyers different prices for essentially the same product or service. H. R Varian, *Price discrimination*, 1 *HANDB. IND. ORGAN.* 597-654 (1989); It is a long-established practice that has greatly increased in frequency as the result of technological advances. Andrew Odlyzko, *Privacy, economics, and price discrimination on the Internet*, in *PROCEEDINGS OF THE 5TH INTERNATIONAL CONFERENCE ON ELECTRONIC COMMERCE* 355-366 (2003) Price discrimination requires sorting buyers into groups according to their willingness to pay, and that requires a significant amount of information. Consequently, sellers structure their interactions so that they can collect and use the necessary information.

interconnections. In the mid-twentieth century, the web created by data distribution was not particularly intricate. This was primarily a function of the available technology, not of norm-imposed prohibitions.

Role-appropriate informational norms allow the distribution of information to third parties. It is, for example, role appropriate for teachers to convey relevant information about students to suitable third parties.<sup>58</sup> Students need information about their academic performance passed on to other institutions and employers, and teachers want to transfer that information so that their students can secure the benefits they merit. These interests only partially overlap. Students have an incentive to present themselves as favorably as possible while their teachers have an incentive to offer a more balanced view to maintain credibility. The norm coordinates these interests in ways that more or less ensure teachers and students appear to each other in ways consistent with those roles, including appearances to third parties. Students, for example, need to know roughly what is in and out of bounds in a recommendation, so they have some approximate idea of how they will appear to other institutions and employers. The idea is “approximate” because there is considerable indeterminacy in what the norm permits. It is typically relevant in a recommendation to mention that the student is highly motivated, and it can be relevant to describe a key event that illustrates and explains the motivation (“So-and-so is committed to being a District Attorney because . . .”). But how deeply can a teacher delve into, or speculate about, the roots of the motivation? It is almost certainly not appropriate to address intimate details of the student’s family relationships (“In my opinion it is her relationship with

---

<sup>58</sup> Wisconsin Department of Public Instruction, *STUDENT RECORDS AND CONFIDENTIALITY* (2013), [http://ssp.wisconsin.gov/ssp\\_srconfid03](http://ssp.wisconsin.gov/ssp_srconfid03); Staff and student confidentiality, *ASSOCIATION OF TEACHERS AND LECTURERS* (2013), <https://www.atl.org.uk/help-and-advice/school-and-college/staff-student-confidentiality.asp>; Jonita Davis, *TEACHERS’ RESPONSIBILITIES FOR STUDENT CONFIDENTIALITY* eHOW, [http://www.ehow.com/info\\_8700551\\_teachers-responsibilities-student-confidentiality.html](http://www.ehow.com/info_8700551_teachers-responsibilities-student-confidentiality.html).

her alcoholic mother that . . .”). Just how much a teacher can delve into a student’s psychological makeup and background in a recommendation letter is a question without a determinate answer.

As with collection and use, the indeterminateness did not matter all that much fifty years ago. Limited distribution meant that any profile that did make its way into the hands of third parties did not make its way into all that many hands. Individuals still retained enough control to selectively disclose information in the ways they wished—more or less. Students could to some extent ensure that different third parties had different views.

So the result is essentially the same as in the restaurant and employment application examples. The relatively limited distribution of information made indeterminateness inconsequential and ensured that individuals retained significant control over information about them. Norm-implemented tradeoffs secured a range of benefits from distributing information but protected privacy by imposing distributional constraints and thus created the selective disclosure required for privacy in public.

#### E. The Power Shift and the Tradeoff Challenge

This pattern of individual control over data no longer holds. People have lost control over their information and have done so in ways that undermine privacy in public. The power to control consumers’ information has shifted to businesses.<sup>59</sup> Not only have advances in

---

<sup>59</sup> Richard Posner’s summary is succinct and accurate:

Until quite recently the information that people voluntarily disclosed to vendors, licensing bureaus, hospitals, public libraries, and so forth, was scattered, fugitive (because the bulkiness of paper records usually causes them to be discarded as soon as they lose their value to the enterprise), and searchable only with great difficulty. So although one had voluntarily disclosed private information on innumerable occasions to sundry recipients, one retained as a practical matter a great deal of privacy. But with digitization, not only can recorded information be retained indefinitely at little cost, but also the information held by different merchants, insurers, and government agencies can readily be pooled, opening the way to assembling all the recorded information concerning an individual in a single digital file that can easily be retrieved and

information processing greatly enhanced collection, use, and distribution, but also individuals have voluntarily placed massive amounts of personal information in the hands of private businesses.<sup>60</sup>

Businesses exploit this shift to resolve boundary questions in *their* favor. This creates a debased form of norm-governed “coordination” that undermines privacy in public instead of creating it. In addition, businesses develop novel forms of interaction for which there are no relevant informational norms at all, and thus a complete absence of the norm-governed coordination essential to privacy in public. This double loss of coordination is a key event in the decline of privacy that began in the mid-twentieth century.

The way to restore adequate privacy in public is to create appropriate informational norms. This involves three tasks. First, since solving a problem requires understanding it, it is necessary to gain a deeper understanding of how technological advances disrupt norm-created coordination. Second, implementing new norms means implementing new norm-created tradeoffs. The tradeoff problem is complex. In the age of Big Data, information processing yields an increasingly large range of benefits associated with an increasingly broad range of risks.<sup>61</sup> Third, it is necessary to develop effective, sufficiently rapid ways to create norms that implement the tradeoffs. We focus on the first task, understanding the loss of coordination.<sup>62</sup> This requires

---

searched. It should soon be possible—maybe it is already possible—to create comprehensive electronic dossiers for all Americans, similar to the sort of dossier the FBI compiles when it conducts background investigations of applicants for sensitive government employment or investigates criminal suspects. The difference is that the digitized dossier that I am imagining would be continuously updated.

Richard Posner, *Privacy, Surveillance, and Law*, 75 UNIV. CHIC. LAW REV. 245, 248 (2008).

<sup>60</sup> See DAVID EASLEY & JON KLEINBERG, NETWORKS, CROWDS, AND MARKETS REASONING ABOUT A HIGHLY CONNECTED WORLD 347 (2010).

<sup>61</sup> See Robert H Sloan & Richard Warner, *Big Data and the “New” Privacy Tradeoff*, BIG DATA PRIV. WORKSHOP PROC. (2013), <http://www.futureofprivacy.org/big-data-privacy-workshop-paper-collection>.

<sup>62</sup> We have addressed the second and third tasks elsewhere. SLOAN AND WARNER, *supra* note 41.

an explicit analysis of norms. We begin with a definition of norms in general and then turn specifically to coordination norms.

### III. NORMS AND COORDINATION

We define norms in terms of nearly complete conformity.<sup>63</sup> A *norm* is a behavioral regularity in a group, where the regularity exists at least in part because almost everyone thinks that he ought to conform to the regularity.<sup>64</sup> We leave open the question of how many must conform for almost everyone in a particular group to conform, as well as the question of how to define the group within which conformity occurs (“almost everyone” means “almost everyone in such-and-such group”). For example, in Jones’s small town, the norm is to go to the Protestant church on Sunday: everyone goes to a Protestant church on Sunday, and they do so at least in part because each believes he or she ought to.

---

<sup>63</sup> We discuss norms in detail in *Id.*

<sup>64</sup> Our notion of a norm is a standard one in recent law and economics literature, with one exception. We explain conformity to the norm by appeal to people’s beliefs above what they ought to do. The recent literature in contrast explains conformity as the result of self-interested actors avoiding the costs of nonconformity. “[One] approach typically assumes that people care only about their own (material) well being, and rely on repeated game models to explain how they cooperate or refrain from violating social norms. . . . [A] second approach typically assumes that people care about something else aside from material goods—esteem, or status, or conformity, or some such thing.” Eric A. Posner, Introduction to SOCIAL NORMS, NONLEGAL SANCTIONS, AND THE LAW xi-xii (Eric A. Posner ed., 2007). Richard McAdams, a proponent of the second approach, notes that “by *norm* I mean a decentralized behavioral standard that individuals feel obligated to follow, and generally do follow . . . [to gain the esteem of others], or because the obligation is internalized, or both.” Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, in SOCIAL NORMS, NONLEGAL SANCTIONS, AND THE LAW 101, 144 (Eric A. Posner ed., 2007). The emphasis on “feeling obligated” would appear close to our view that people conform because they think they ought to; however, McAdams explains “feeling obligated” in terms of the costs of non-conformity—thus: “Without internalization, one obeys the norm to avoid external sanctions. . . . After internalization, there is yet another cost to violating a norm: guilt. The individual feels psychological discomfort whether or not others detect her violation.” *Id.* McAdams still conceives of people as self-interested agents seeking to avoid costs they regard as unacceptable. We take it to be clear that people are not merely self-interested agents. The assumption that they are has been extensively and decisively criticized. *See, e.g.*, AMARTYA SEN, THE IDEA OF JUSTICE 32-33 (2009).

A. Coordination Norms

Like norms generally, a coordination norm is a behavioral regularity in a group to which people conform because they think they ought to do so. The difference is that people think they ought to conform because, and only as long as, they think almost everyone else will. This is not true of the church example: people could and would attend church even if others did not. Driving on the right is the classic example of a coordination norm. People drive on the right because, and only as long as, almost everyone else does so.<sup>65</sup> You would not drive on the right if you expected everybody else to drive on the left. Safety and convenience dictate that you drive on the same side as everyone else, and you need to coordinate with the others' cooperation to do that. Thus our definition of a coordination norm: a coordination norm is a behavioral regularity in a group, where the regularity exists at least in part because almost everyone thinks that, in order to realize a shared interest, she ought to conform to the regularity, as long as everyone else does.<sup>66</sup>

Entering an elevator occupied by others is a good example. The norm is to maximize the distance to your nearest neighbor.<sup>67</sup> All share an interest in being able to use the elevator and avoiding overcrowding, and no one can realize the interest unilaterally. Elevator users think they ought to conform to achieve this balance—as long as everyone else does so. There is little point in being a “nearest-neighbor distance maximizer” if everyone else just stands wherever they like.

---

<sup>65</sup> H. Peyton Young, 10 J. ECON. PERSPECT. 105, 107–108 (1996) (providing a game-theoretic explanation of the decision made by individual drivers as to whether to drive on the right or left side of the road).

<sup>66</sup> See SLOAN AND WARNER, *supra* note 41 at 56 – 59.

<sup>67</sup> This is a simplification. The true norm is closer to “maximize the distance from your nearest neighbor subject to the constraint that you stay within the peripheral vision of at least one other passenger, and that you have at least one other passenger within your peripheral vision.” See Matthew Solle, WHERE WE STAND IN AN ELEVATOR, YOU THE USER (2012), <http://www.youtheuser.com/2012/04/26/where-we-stand-in-an-elevator/> (last visited Feb 9, 2014).

The informational norms that facilitate the coordination essential to privacy in public are coordination norms.<sup>68</sup> People coordinate to create privacy in public in just the way they coordinate driving on the right—through a coordination norm. The examples in the last section exhibit the key features of coordination norms. There is a shared interest (meeting needs, fitting with the job, presenting a balanced view of a student’s performance). In addition, the parties conform to the prevailing interpretation of the norm only as long as they think the other parties will conform. If, for example, most customers insisted that restaurants provide them with a detailed questionnaire about their food preferences every time they went to a restaurant, restaurants would comply to get the business and the remaining minority of customers would most likely continue to patronize survey-supplying restaurants to get the food. Similarly, if most job applicants or students preferred employers and schools that accepted the applicants’ or students’ recent Myers-Briggs personality test results, employers and schools would accept the results.<sup>69</sup>

#### B. Value-Optimality and Privacy in Public

A cornerstone of our account is the notion of a *value-optimal* norm. Only *value-optimal* norms create adequate privacy in public. Technology-driven business practices undermine privacy in public by creating situations that are not governed by value-optimal norms—either by causing existing norms to cease to be value-optimal, or by creating situations for which there are no relevant norms and so no value-optimal ones. We begin by defining value-optimality.

---

<sup>68</sup> Not all informational norms are coordination norms. “Make your comments relevant” is an informational norm, but not a coordination norm. The hallmark of a coordination norm is that you adhere to it *only* as long as others do, but you would adhere to the relevant comment norm even if most others did not.

<sup>69</sup> For a fuller argument, see SLOAN AND WARNER, *supra* note 41, which discusses similar examples of changes in consumers’ demands. The discussion proceeds in terms of the “consumers only” formulation of norms explained *supra* note 41, a formulation which proves advantageous in this context.

A norm is value-optimal when, in light of the values of all (or almost all) members of the group in which the norm obtains, the norm is at least as well justified as any alternative.<sup>70</sup> A norm that is at least as well justified as any alternative is either better justified than any alternative or is tied with one or more alternatives that are also better than the rest. This is why it is appropriate to call a norm *value-optimal* when it is at least as well justified as any alternative norm: there is no better alternative.<sup>71</sup>

We will focus primarily on norms that are not value-optimal. A classic example is the “no helmet” norm among National Hockey League players.<sup>72</sup> Before 1979, not wearing a helmet was a behavioral regularity that existed in part because each player thought he ought to conform—*as long as all the others did*. Wearing a helmet meant not looking tough, and involved a slight loss in peripheral vision. However, each player would have happily worn a helmet if he thought almost all the others were going to. Because of the value they placed on avoiding head injuries, virtually all the players regarded the alternative in which they all wore helmets as better justified. Thus, the no-helmet norm was not value-optimal. But the players remained trapped in it because no individual player would wear a helmet as long as he expected most others not to.<sup>73</sup>

Consumers “play privacy without a helmet” when informational norms cease to be value-optimal. Lack of value-optimality means: either too much privacy and too little information

---

<sup>70</sup> To avoid misunderstanding, we should note that we are not, for example, saying that when you step into an elevator, you explicitly think about where you ought to stand. Typically, people just unreflectively conform to the norm. The point is that you could justify conformity if you reflected on the norm under ideal conditions (including having sufficient time, sufficient information, lack of bias, and so on).

<sup>71</sup> There are many optimality notions; Pareto optimality is perhaps the most well-known. A situation is Pareto-optimal when, and only when, it is not possible to improve the well-being of any one person without making others worse off. Value-optimality is an ideal that we approximate in practice. We want our norms to be close enough to being value-optimal. We will throughout for convenience drop the “close enough to being” qualification and just refer to norms as value-optimal or not.

<sup>72</sup> We have discussed the example before in SLOAN AND WARNER, *supra* note 41 at 61 – 62; The original source is T. C. Schelling, *Hockey Helmets, Concealed Weapons, and Daylight Saving: A Study of Binary Choices With Externalities*, 17 J. CONFL. RESOLUT. 381 (1973).

<sup>73</sup> See Schelling, *supra* note 72 at 381.

processing; or, too little privacy and too much information processing. Technology-driven business information processing practices pass significant control over consumers' information to businesses in ways that create an extreme case of too little privacy and too much information processing, and consumers remain trapped in a norm that, contrary to their values, undermines rather than creates privacy in public. This debased "coordination" combines with a total lack of relevant norm implemented coordination in those cases in which innovative practices have outstripped the relatively slow pace of the formation of norms. The combination significantly erodes privacy in public, and, to the extent it disappears, multifaceted selves face the threat of disappearing—literally—from the scene.

In both cases, the solution is to create new norms, and that means identifying value-optimal tradeoffs between informational privacy and the benefits of information processing. One problem is that value-optimal tradeoffs are not always already contained in our values just waiting for us to think long enough and hard enough to find them. Defining value-optimal tradeoffs is not like looking for buried treasure. The treasure is there whether you find it or not, but in creating new norms it will often be necessary to *invent* the tradeoffs. The reason is that values are not closed, complete, consistent systems that guide you through all decisions you must make. Instead, they are often more or less detailed outlines that leave large areas barely filled in, and they may incorporate competing, or outright inconsistent, claims and views, whose weight is not fixed in advance of reasoning about particular situations.

We focus first on existing norms that have lost value-optimality and then turn to the cases of a complete lack of relevant norms.

#### IV. THE EROSION OF PRIVACY IN PUBLIC: THE LOSS OF VALUE-OPTIMALITY

Businesses transform value-optimal norms into ones that are not through technology-driven businesses practices that occupy the norm's indeterminate areas. We describe three examples—one each for collection, use, and distribution.

A. Collection: Anybody Can Know About Anybody

Imagine a mythical small town in which *everyone* really does know *everyone* in great detail. Information technology has not even come close to creating a small town in this sense. Most of the 316 million people in the United States<sup>74</sup> know *nothing* about the vast majority of those millions. It takes time, effort, and money to collect and use information in that way, and only those who see the payoff as greater than the effort will select some people to investigate. Information technology and the Internet ensure that almost anybody can find out a great deal about almost anybody. And people do—for example: journalists, skip tracers, people going on dates, email providers, politicians, security experts, bankers, lawyers, and jury analysts.

The restaurant example is a good illustration of the effect of merely knowing.<sup>75</sup> The journalist Jason Heidemann describes his recent visit to Goosefoot,

chef Chris Nugent's ballyhooed restaurant in Lincoln Square . . . I'd barely sat down when [co-owner and host Nina] began making informed references about me—specifically my job. I recall her asking how long I'd been there and what projects was I working on. When I pressed her, she confessed she had Googled me in advance of my visit. At Chicago's best restaurants, this has become increasingly common.<sup>76</sup>

Google is far from the only source of information restaurants now have. The online reservation service Open Table, for example, allows “sommeliers and maitre d’s [to] use the system to easily

---

<sup>74</sup> United States Census Bureau, U. S. AND WORLD POPULATION CLOCK, <http://www.census.gov/popclock>.

<sup>75</sup> You might consider the restaurant example to instead illustrate the combined effect of knowing and using. However, our point is that once one merely knows, certain use becomes more or less automatic, requiring no additional effort.

<sup>76</sup> Jason A. Heidemann, YOU’VE BEEN GOOGLED — BON APPETIT!, CRAIN’S CHICAGO BUSINESS (2013), <http://www.chicagobusiness.com/article/20130629/ISSUE03/306299997/#>.

catalog diners' habits and quirks, resulting in a vast database of customer information."<sup>77</sup> Other data aggregation and analysis services for restaurants abound.<sup>78</sup> Is it role appropriate for restaurants to acquire such data? The indeterminateness in the norm-drawn boundaries means that there is no clear answer. Businesses practices move into the indeterminate area. This gives rise to the four-part pattern, we describe below. Similar patterns characterize the use and distribution examples we examine later, and we suggest the pattern is characteristic of cases in which norms cease to be value-optimal.

(1) *Businesses treat the practice as role appropriate.* Restaurants defend their data collection as simply a better way to do what they have always done, meet customers' needs. One commentator notes that "[f]or many restaurateurs, today's detailed dossiers are merely a modern spin on the old fashioned, high-touch service associated with legendary hosts such as Niccolini and Sirio Maccioni, who's been running Midtown's storied Le Cirque restaurant since 1974."<sup>79</sup> As one restaurateur put it, "There's a fine line, but as long as you don't cross it, people just think you're good at your job."<sup>80</sup> Such attitudes should come as no surprise. As James Rule notes,

Aware of it or not, we are all heirs to potent Enlightenment ideas in matters relating to control. If knowledge is good, and informed action preferable to the alternative, why shouldn't we expect institutions of all kinds to maximize their grip on the lives of those they deal with? If government and private organizations are pursuing what are publicly recognized as legitimate ends, why shouldn't they do so as efficiently as possible?<sup>81</sup>

The theme that "knowledge is good, and informed action preferable to the alternative" runs through the next two examples as well.

---

<sup>77</sup> Carla Spartos, *Is your restaurant spying on you?*, NEW YORK POST, December 22, 2010, <http://nypost.com/2010/12/22/is-your-restaurant-spying-on-you/>.

<sup>78</sup> See Stephanie Miles, 6 TOOLS RESTAURANTS CAN USE FOR BETTER GUEST INTELLIGENCE, STREETFIGHT (2103), <http://streetfightmag.com/2013/07/22/6-tools-restaurants-can-use-for-better-guest-intelligence/>.

<sup>79</sup> Spartos, *supra* note 77.

<sup>80</sup> *Id.*

<sup>81</sup> RULE, *supra* note 1 at 192.

(2) *Consumers object to the invasion of privacy.* The “fine line” comment reveals the problem. The lines norms draw are not *fine* but indeterminate; moreover, it is no longer the customer who decides what tradeoffs occur in those indeterminate regions, it is the restaurant. This deprives customers of control that they had until recently over how they appear. Some customers might be quite willing to trade some control for restaurants being better able to meet their needs, but even those customers have no control over the tradeoff, the restaurants do. This loss of control is a loss of informational privacy, and customers object to the loss. When Heidemann “posted a note about the trend [of restaurants Googling customers] on . . . a message board for Chicago foodies,” the responses ranged from “That’s just odd” to “I would like to know which restaurants research their clientele, so I make sure I never go there.”<sup>82</sup> The objections are hardly a surprise. Over twenty years of studies and surveys show that consumers want more control over their data than current business information processing practices provide.<sup>83</sup> In addition, it is *the restaurants* making tradeoff decisions about privacy for their customers, and those decisions are bound to provoke objections. As James Rule notes,

[M]any people seem to identify the point at which routine claims on personal information cross the line into intolerable privacy invasion in much the same way most people classify pornography: they know it when they see it. But as with pornography, reasonable people often disagree on where to draw the line. One man’s shameless exploitation of sex

---

<sup>82</sup> Heidemann, *supra* note 76.

<sup>83</sup> Alessandro Acquisti & Jens Grossklags, *Privacy and rationality in individual decision making*, 3 IEEE SECUR. PRIV. 26–33, 28 (2005) A typical study found that 89% of consumers had either a “high concern” (53.7%) or a “medium concern” (35.5%) about “general privacy.” Of course, finding that consumers are “concerned” does not mean that they are concerned about loss of control over their information, but why else would they be concerned? The worry is surely that others will do something unacceptable, so consumers must be concerned about some combination of the intertwined issues of trust and control. It would indeed be strange if this were not true. In general, control and trustworthiness are important considerations in determining whether to enter or continue a relationship; we may, for example, refuse to work with, go on a trip with, or associate with someone because he or she is too controlling or too untrustworthy. Studies of consumer attitudes toward direct marketing confirm this conclusion. One recent study found that, when consumers are informed about current direct marketing information processing practices, between 73% and 86% find such practices objectionable. JOSEPH TUROW ET AL., *AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT* (2009), <http://ssrn.com/abstract=1478214>.

for profit may turn out to be the next woman's harmless erotica, or even serious art or literature for a third consumer.<sup>84</sup>

(3) *Consumers nevertheless continue to conform to the reinterpreted norm.* Customers continue to go to restaurants that engage in intensive data collection. This may provoke the response, “Of course, because most do not understand what the restaurants are doing.” But, even if they did understand, many would still patronize data-collecting restaurants. Privacy is only one factor in a choice of a restaurant. The quality and type of food, the service, ambience, price, and location matter a great deal, and people are remarkably ready to trade privacy for other benefits.<sup>85</sup> Lack of choice is another reason. An ever increasing number of restaurants collect data about their customers.<sup>86</sup> Competition among restaurants is fierce, and many restaurateurs believe that intensive data collection gives them a competitive edge.<sup>87</sup> It takes time and effort to investigate a restaurant’s information processing practices, and we “give up data about ourselves because we don’t have the time, patience, or single-mindedness about privacy that would be required to live our daily lives in another way.”<sup>88</sup>

---

<sup>84</sup> RULE, *supra* note 1 at 146.

<sup>85</sup> While a large number of studies show that consumers are concerned about losing control over personal information, “a number of . . . recent surveys, anecdotic evidence, and experiments . . . have . . . shown that individuals are actually less concerned about privacy than what they claim to be: many are willing to provide very personal information, in exchange for small rewards.” Alessandro Acquisti, *Privacy and Security of Personal Information*, in *ECONOMICS OF INFORMATION SECURITY* 179–186 (J. Camp & R. Lewis eds., 2004). This may seem inconsistent with the concern noted *supra* note 83 to have more control over information. We think the inconsistency is only apparent. We explain the willingness to “trade cheaply” as just the behavior to be expected from people trapped in an informational norm that is not value-optimal. SLOAN AND WARNER, *supra* note 41, at 101 - 102.

<sup>86</sup> See Your favorite restaurant could be stalking you, EXAMINER.COM (2012), <http://www.examiner.com/article/your-favorite-restaurant-could-be-stalking-you> (last visited Feb 9, 2014); Mariani, *supra* note 45.

<sup>87</sup> See Your favorite restaurant could be stalking you, *supra* note 85 (noting the “competitively fierce restaurant environment” and the increased use of tracking technology). See also You do have a customer database, don’t you?, O’DELL RESTAURANT CONSULTING’S BLOG, <http://blog.bodellconsulting.com/2008/01/15/you-do-have-a-customer-database-dont-you/> (last visited Feb 9, 2014).

<sup>88</sup> HAL ABELSON, KEN LEDEEN & HARRY LEWIS, *BLOWN TO BITS: YOUR LIFE, LIBERTY, AND HAPPINESS AFTER THE DIGITAL EXPLOSION* 41–42 (2008).

(4) *The norm is not value-optimal.* The norm is not value-optimal if there is a better justified alternative, and consumers think there is—one with a more restrictive interpretation of role-appropriate data collection that gives them more control over their information. There is excellent empirical and theoretical reason to think this is true. The empirical reason consists of the over twenty years of studies that show that consumers desire more control over their data.<sup>89</sup> The theoretical reason is that an adequate degree of privacy in public is essential to the realization of a multifaceted self. Ensuring that conditions allow you to be who you are is certainly an excellent reason for the concern with control.

#### B. Allocation of Risks and Benefits

Modern data collection and analysis greatly increases the power of private businesses to determine the distribution of goods, services, and employment. The concern is not that private businesses have the power to distribute such benefits. Their having some degree of power to do so is a defining feature of a market economy. The concern is that the power is now too great. One problem is that the resulting distributions of costs and benefits are sometimes unjust, as we have argued elsewhere.<sup>90</sup> Here we focus on the effect on multifaceted selves. Enhancing the power to make fine-grained distinctions in the distribution of costs and benefits increases the incentive to make sure you stay in the straightjacket of exhibiting the characteristics businesses reward.

Employment background checks are a good example. Job applicants are only one source of information for employers. HireRight and Lexis/Nexis, for example, offer to search county, state and federal criminal records, national criminal database records, international criminal

---

<sup>89</sup> Acquisti, *supra* note 85.

<sup>90</sup> SLOAN AND WARNER, *supra* note 41.

records, civil court records, the national theft database, drug and alcohol databases, motor vehicle records, and ex offender registries. Its services also include verifying Social Security Numbers, employment, education, professional licenses, professional credentials verification; it will also provide professional reference checks and credit reports.<sup>91</sup> “Screening often goes far beyond the familiar checking of public criminal records. For \$60 to \$80 per applicant, ChoicePoint [now Lexis/Nexis] and its rivals assemble digital dossiers of educational degrees and credit histories as well as interviews with friends, past bosses, and colleagues.”<sup>92</sup> Employers can discover additional information on their own by Googling applicants, visiting their social networking sites, or using sites like PeekYou<sup>93</sup> and Spokeo.<sup>94</sup> Does this degree of penetration into people’s personal lives violate a role-appropriate informational norm? It is, within limits, role appropriate for an employer to collect and use information that will help determine how well a job applicant will fit the needs of the business. The limits are sufficiently indeterminate that employers can with some plausibility claim that intensive background checks are role appropriate. The pattern that arises is the same as in the restaurant example.

(1) *Businesses treat the practice as role appropriate.* Businesses sound the “knowledge is good, and informed action preferable to the alternative” theme and treat background checks as just an improvement on the well-established practice of determining how well an applicant will fit with the job. One recent defense of background checks argues that “background checks help

---

<sup>91</sup> See Background Screening, HIRERIGHT, <http://www.hireright.com/Background-Checks.aspx?apsi=0>. <http://www.lexisnexis.com/backgroundchecks>.

<sup>92</sup> Chad Terhune, THE TROUBLE WITH BACKGROUND CHECKS BLOOMBERG BUSINESS WEEK MAGAZINE (2008), <http://www.businessweek.com/stories/2008-05-28/the-trouble-with-background-checks>.

<sup>93</sup> <http://www.peakyou.com/usa>. See Bob Rankin, IS PEEK YOU EVIL? ASK BOB RANKIN, [http://askbobrankin.com/is\\_peakyou\\_evil.html](http://askbobrankin.com/is_peakyou_evil.html). (links may include social networking profiles).

<sup>94</sup> [www.spokeo.com](http://www.spokeo.com). See Justin Brookman, COMPLAINT TO THE FTC IN THE MATTER OF SPOKEO CENTER FOR DEMOCRACY AND TECHNOLOGY, <https://www.cdt.org/comments/complaint-ftc-matter-spokeo> (“profiles include highly personal information, including religious and ethnic background, judgments about shopping and recreational habits, and information about family members and roommates”).

employers make better hiring decisions. With screening, we can learn about the past behaviors and experiences of an individual in order to make informed predictions about how well an employee will perform inside our organization.”<sup>95</sup> Similarly, the City of Bozeman, Montana defended its practice of requiring social networking site passwords from applicants by insisting that

“[b]efore we offer people employment in a public trust position, we have a responsibility to do a thorough background check . . . Shame on us if there was information out there available about a person who applied for a job who was a child molester or had some sort of information out there on the Internet that kind of showed those propensities and we didn't look for it, we didn't ask, and we hired that person.”<sup>96</sup>

There are many similar examples.

(2) *Applicants object to the invasion of privacy.* Pre-employment background checks have caused a storm of protest.<sup>97</sup> The Bozeman city's defense of insisting on social networking passwords, for example, “wasn't good enough for many critics, who cited the move as an invasion of privacy. After the story was covered in the local news, residents sent hordes of letters and e-mails to city hall, eventually forcing officials to back down and discontinue the practice.”<sup>98</sup>

(3) *Applicants nonetheless continue to conform to the norm under employers' new interpretation of role appropriateness.* Employer use of background checks is widespread, so not complying with employer background checks would mean not applying for employment in a significant range of cases.

---

<sup>95</sup> Evan Carmichael, WHERE DO YOU STAND ON EMPLOYMENT BACKGROUND CHECKS?, BELIEVE, <http://www.evancarmichael.com/Human-Resources/5885/Where-Do-You-Stand-on-Employment-Background-Checks.html>.

<sup>96</sup> 37 Percent Of Employers Use Facebook To Pre-Screen Applicants, New Study Says, HUFF POST BUSINESS (2012), [http://www.huffingtonpost.com/2012/04/20/employers-use-facebook-to-pre-screen-applicants\\_n\\_1441289.html](http://www.huffingtonpost.com/2012/04/20/employers-use-facebook-to-pre-screen-applicants_n_1441289.html).

<sup>97</sup> Terhune, *supra* note 92; Pre-Employment Background Checks, U. S. SMALL BUSINESS ADMINISTRATION SBA.GOV, <http://www.sba.gov/content/pre-employment-background-checks>; Privacy in Employment Law, Fourth Edition, BLOOMBERG BNA, <http://www.bna.com/privacy-employment-law-p17179869438/> (last visited Feb 8, 2014).

<sup>98</sup> 37 Percent Of Employers Use Facebook To Pre-Screen Applicants, New Study Says, *supra* note 96.

(4) *The norm so interpreted is not value-optimal.* There is a better justified alternative. The reason is the same as in the restaurant example: empirical studies establish people's desire for more control over their information and, moreover, that control is essential to realizing a multifaceted self. In this case, however, there is an additional reason: namely, to create a better distribution of employment than the one created by the current use of pre-employment background checks. A better distribution is called for because the current distribution strongly discriminates against "undesirable" applicants—applicants that impose significant risk or cost on the employer. Imagine, for example, that Alice is a single mother whose three-year old child has a severe chronic illness requiring long-term expensive treatment. Alice will potentially increase an employer's health care costs and will have a greater than normal number of absences from work. She is, in this sense, an "undesirable" hire. This is inconsistent with (most) people's values. One reason, and the one most pertinent here, is that the practice works against the realization of multifaceted selves by creating a very strong incentive to make sure that the shape of your life takes is one employers find desirable, not one that reflects who you are. This is the twenty-first century version of the high school teacher's threat, "This will go on your permanent record." As one blogger notes, "Every classroom contains a few kids who are bored and like to cause trouble. When I was in school, our teachers would threaten them by saying, 'This will go on your permanent record!' *The threat was effective*: none of us wanted to be prevented from going to college or from getting a job."<sup>99</sup>

In short, the second reason the new norm for hiring practices is not value-optimal is that the resulting distribution of jobs is unjust. At least, *we* think so, and we assume many if not most

---

<sup>99</sup> See Mike Pilewski, SURPRISE! YOUR BEHAVIOR IS ON RECORD (2010), <http://www.spotlight-online.de/blogs/mike-pilewski/surprise-your-behavior-is-on-record> (emphasis added). See also Peter Anthony Holder, THIS WILL GO ON YOUR PERMANENT RECORD, PETER ANTHONY HOLDER'S "STUPH FILE" (2011), <http://peteranthonyholder.blogspot.com/2011/03/this-will-go-on-your-permanent-record.html>.

agree. We assume that at least some types of “undesirable” hires ought to be employed, and hence that a just distribution of employment requires a distribution of those “undesirable” employees over employers in a way that reasonably spreads the increased costs and risks over employers as a whole. This more or less happened in the mid-twentieth century. It was difficult for employers to discover, for example, that Alice was a single mother with a sick child if she did not disclose that, and the same was true for a wide range of other “undesirable” traits. The result was in effect a lottery: the luck of the draw distributed employees with “undesirable” traits over employers as a whole. Now, to continue with Alice, information aggregators may easily pick up her Internet activities (visits to health care sites, support forums, Facebook postings, and the like) and flag her as a risk for significant work absences and high health care costs. Swap the sick child for a criminal record, a bad credit history, being a recovering alcoholic, having had an episode of depression requiring prescription drugs, or any other trait some employer finds objectionable. The result is a profound—and unjust—change in the distribution of employment.<sup>100</sup>

---

<sup>100</sup> See Beth Givens, PUBLIC RECORDS ON THE INTERNET: THE PRIVACY DILEMMA, PRIVACY RIGHTS CLEARING HOUSE (2002), <https://www.privacyrights.org/ar/onlinepubrecs.htm> Indeed, it is possible that our society will see “a growing number of individuals who are disenfranchised for life. Large numbers will not be able to find employment because of negative information . . .—whether true or not—from years gone by. Or they will be relegated to lower-paying jobs in the service industries, unable to bring their true abilities into the employment marketplace.” Further, “Nearly 1 in 4 adults (an estimated 65 million people) in the U.S. have a criminal record, and more are mistakenly identified as having one.” Broken Records: How Errors by Criminal Background Checking Companies Harm Workers and Businesses (Summary), NATIONAL CONSUMER LAW CENTER (2012). Nationally, African Americans and Hispanics are arrested in numbers disproportionate to their representation in the general population. In 2010, 28% of all arrests were of African Americans, even though African Americans only comprised approximately 14% of the general population. In 2008, Hispanics were arrested for federal drug charges at a rate of approximately three times their proportion of the general population. EEOC Enforcement Guidance, No.915.002, U. S. EQUAL OPPORTUNITY ENFORCEMENT COMMISSION (2012), [http://www.eeoc.gov/laws/guidance/arrest\\_conviction.cfm#V](http://www.eeoc.gov/laws/guidance/arrest_conviction.cfm#V). It is not just criminal records that matter. Any trait an employer might find objectionable is relevant. See Joseph Walker, *Do New Job Tests Foster Bias?*, THE WALL STREET JOURNAL, September 20, 2012, <http://online.wsj.com/article/SB10000872396390443890304578006283936708970.html>.

Similar remarks apply to health insurance,<sup>101</sup> the extension of credit,<sup>102</sup> direct marketing,<sup>103</sup> price discrimination,<sup>104</sup> and news reporting.<sup>105</sup> We acknowledge—indeed emphasize—that there are significant differences among the examples. Each merits and requires detailed examination on its own; in particular, the analysis of the loss of value-optimality will vary considerably in each case and this means that the task of creating relevant value-optimal norms differs in each case.

### C. Distribution

Distribution multiples collection and use by turning the simple hub-and-spoke structure created by an initial instance of data collection into a web of interconnections. The combination of modern information processing techniques and the Internet mean that distribution now creates vastly more interconnections than it did in the past. For example, one of us recently visited the chess website, chess.com. The site collects information for its purposes and also serves as a conduit for the transfer of information to third parties. The visit produced the following

---

<sup>101</sup> See SLOAN AND WARNER, *supra* note 41 at 107 – 109.

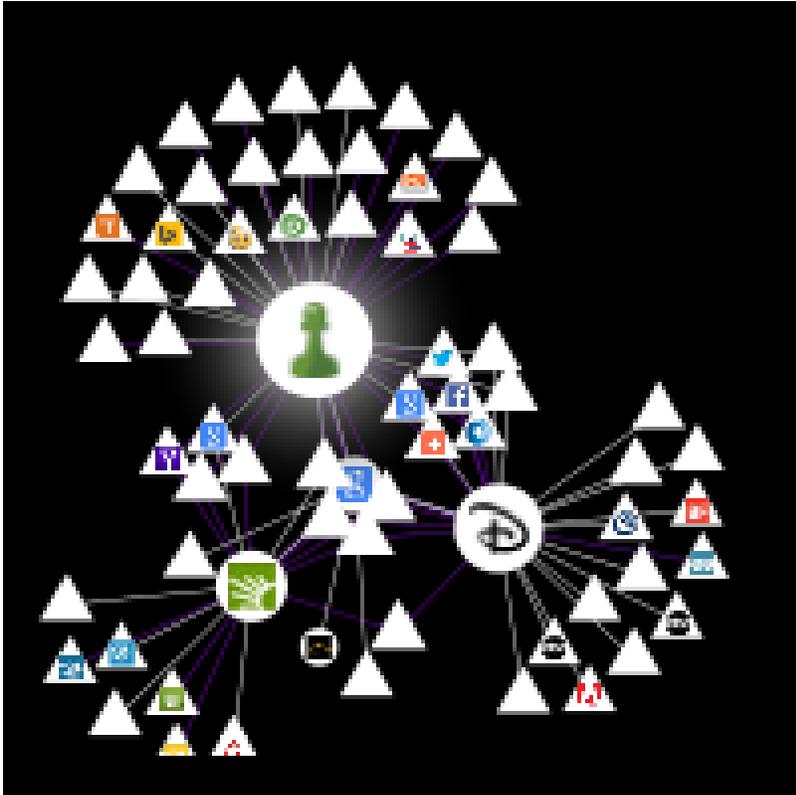
<sup>102</sup> See James Rule's discussion of the greatly enhanced ability of creditors to determine whether their criteria of credit worthiness are fulfilled. RULE, *supra* note 1 at 103. See also Andy Oram, CREDIT CARD COMPANY DATA MINING MAKES US ALL INSTANCES OF A TYPE, O'REILLY RADAR, <http://radar.oreilly.com/2009/05/credit-card-company-data-minin.html> (last visited Feb 14, 2014); Charles Duhigg, *What Does Your Credit-Card Company Know About You?*, NEW YORK TIMES MAGAZINE, May 12, 2009, <http://www.nytimes.com/2009/05/17/magazine/17credit-t.html>.

<sup>103</sup> SLOAN AND WARNER, *supra* note 41 at 96 - 102.

<sup>104</sup> Price discrimination and its data collection practices are controversial. Andrew Odlyzko, *Privacy and the clandestine evolution of e-commerce*, in ICEC '07: PROCEEDINGS OF THE NINTH INTERNATIONAL CONFERENCE ON ELECTRONIC COMMERCE 3–6 (2007). The ways in which online businesses sort customers for purposes of price discrimination is an interesting question. See Arvind Narayanan, *ONLINE PRICE DISCRIMINATION: CONSPICUOUS BY ITS ABSENCE, 33 BITS OF ENTROPY*, <http://33bits.org/2013/01/08/online-price-discrimination-conspicuous-by-its-absence/> (last visited Feb 15, 2014)(distinguishing among overt and concealed price discrimination and product discrimination).

<sup>105</sup> Technology has both expanded reporters' access to information and their ability to report it through non-traditional means such as blogs. The greatly increased depth to which reporters can penetrate into people's lives is highly controversial. JON L MILLS, *PRIVACY: THE LOST RIGHT* 287 (2008).

pattern.<sup>106</sup> The triangles are third party sites collecting, using, and distributing information; chess.com is the circle with the pawn, and the other circles are previously visited sites:



This picture is just a partial representation of the actual structure. A more detailed picture would also show transfers from the third parties to others that will also collect, use, and distribute the information to others (who may distribute it to others, and so on). The complexity is immense:

The technical and institutional story is so complicated that probably only a handful of deep experts would be able to piece together a full account . . . Even if, for a given moment, a snapshot of the information flows could be grasped, the realm is in constant flux, with new firms entering the picture, new analytics, and new back-end contracts forged: in other words, we are dealing with a recursive capacity that is indefinitely extensible.<sup>107</sup>

---

<sup>106</sup> Generated using LightBeam. “Lightbeam is a Firefox add-on that enables you to see the first and third party sites you interact with on the Web. Using interactive visualizations, Lightbeam shows you the relationships between these third parties and the sites you visit.” Salvatore on February 5 & 2014 · Permalink · Translate, LIGHTBEAM FOR FIREFOX, <https://addons.mozilla.org/en-US/firefox/addon/lightbeam/> (last visited Feb 9, 2014).

<sup>107</sup> Nissenbaum concludes that “the complexity makes it not only difficult to convey what practices are followed and what constraints respected, but practically impossible.” Nissenbaum, *A Contextual*



privacy in public by multiplying the instances of conformity to norms that have lost their value-optimality. This is excellent reason to seek replacement norms with better privacy tradeoffs for restaurants, employers, and businesses. But what about Google, OpenTable, HireRight, Lexis/Nexis, and information aggregators generally? Are there informational norms relevant to assessing their activities? In some cases; in others, technology-driven business innovation creates activities that are not governed by any relevant informational norms at all. We consider one loss of value-optimality example now and turn to the “no norms” cases next.

We take the facts from *Dwyer v. American Express*.<sup>109</sup> American Express analyzed the purchases of its cardholders to divide them into

six tiers based on spending habits and then rent this information to participating merchants as part of a targeted joint-marketing and sales program. For example, a cardholder may be characterized as “Rodeo Drive Chic” or “Value Oriented.” In order to characterize its cardholders, [American Express] analyze[s] where they shop and how much they spend, and also consider behavioral characteristics and spending histories . . . The merchants using the defendants’ service can also target shoppers in categories such as mail-order apparel buyers, home-improvement shoppers, electronics shoppers, luxury lodgers, card members with children, skiers, frequent business travelers, resort users, Asian/European travelers, luxury European car owners, or recent movers.<sup>110</sup>

Dwyer sued—unsuccessfully—for the invasion of his privacy. Our concern, however, is with norms, not laws. Does American Express violate a relevant role-appropriate informational norm? Or does it act role-appropriately? It is, within limits, role appropriate for a business to process information to maintain and improve the business, and, within limits, it is unobjectionable for a business to sell a by-product generated in the course of its other business activities. It is unobjectionable for bakers to sell the by-product of breadcrumbs to pie makers, for example. In this case, however, the by-product consists of consumer profiles sold to direct marketers. Is that

---

<sup>109</sup> *Dwyer v. American Exp. Co.*, 273 Ill App 3d 742 (1995).

<sup>110</sup> *Id.* at 743–744.

role appropriate? The constraints on distribution are sufficiently indeterminate that the answer is at the very least unclear. The pattern is the same as before.

(1) *Businesses treat the practice as role appropriate.* Businesses largely take it for granted that a standard part of their business model consists of processing customer data both for internal use and, depending on the business model, for distribution to third parties. In a report revealingly entitled, *The New Rules Of The Road: Marketing Data Governance In The Era Of “Big Data,”* the Winterberry Group advises that “[e]levating the role of marketing data—especially in organizations that have been driven by the “brand” and other factors that were once considered largely independent from its influence—will substantially affect how enterprises invest in tools, talent, internal processes and other resources that are core to their customer interaction effort.”<sup>111</sup> Indeed, “[t]he past fifteen years have seen extensive investments in business infrastructure, which have improved the ability to collect data throughout the enterprise. Virtually every aspect of business is now open to data collection and often even instrumented for data collection.”<sup>112</sup> The distribution of data for direct marketing is only a small part of the picture. “[V]endors from whales like IBM and HP to pure-plays like Vertica and Cloudera are bringing in significant revenue today helping enterprises, governments and healthcare organizations process and make sense of the torrents of unstructured data flowing from mobile devices, sensors, social media and other sources.”<sup>113</sup>

The remaining three parts of the pattern parallel the earlier examples. (2) *Consumers object to the loss of privacy.* Consumers’ privacy objections and concerns about direct marketing

---

<sup>111</sup> WINTERBERRY GROUP, *THE NEW RULES OF THE ROAD: MARKETING DATA GOVERNANCE IN THE ERA OF “BIG DATA”* 6 (2013), <http://thedma.org/research/>.

<sup>112</sup> FOSTER PROVOST & TOM FAWCETT, *DATA SCIENCE FOR BUSINESS: WHAT YOU NEED TO KNOW ABOUT DATA MINING AND DATA-ANALYTIC THINKING* Kindle Locations 242–244 (2013).

<sup>113</sup> *Big Data Is Big Market & Big Business - \$50 Billion Market by 2017*, FORBES, <http://www.forbes.com/sites/siliconangle/2012/02/17/big-data-is-big-market-big-business/> (last visited Feb 9, 2014).

are well documented.<sup>114</sup> (3) *They nonetheless conform to the norm as newly interpreted by businesses.* Not doing so would mean not dealing with an extremely wide range of business and not using forms of electronic payment. (4) *The norm so interpreted is not value-optimal.* A norm that gave consumers more control over their data would be a better justified alternative.

#### D. Two Ways to “Play Without a Helmet”

As the discussion in this section illustrates, technology-driven business practices occupy the indeterminate regions of norm-drawn boundaries in ways that massively expand the collection, use, and distribution of information. The result is that a variety of informational norms involved are no longer value-optimal and now promote behavior that undermines privacy in public instead of creating it. Consumers do not resist the transformation even though it puts the realization of multifaceted selves at risk. Like the pre-1979 hockey players, they remain trapped in the norms: they “play privacy without a helmet.” They still coordinate with businesses but in ways that undermine the privacy they need. This degraded cooperation is not the only way to “play privacy without a helmet.” Another way is to engage in commercial transactions that are not governed by relevant norms at all. In this case, the helmet has not disappeared; it never existed in the first place.

Advances in information processing combined with new business models have created a wide range of situations that are not governed by relevant informational norms. To see how this happens, consider what is required for an informational norm to exist. There must be a shared concept of role-appropriate information processing. The concept serves as the focal point around which consumers and businesses coordinate with regard to information processing. Shared conceptions of role-appropriateness evolve over time through patterns of social and commercial

---

<sup>114</sup> *See supra* note 83.

interaction, and the process is considerably slower than the rapid proliferation of innovative commercial interactions driven by the rise of the Internet and advances in information processing technology.

There are significant similarities between the “no norms” cases and the loss of value-optimality in existing norms. Both exhibit a similar four-part pattern, and the result is the same in each case: massive collection, use, and distribution erode privacy in public. In light of these similarities, our discussion can be brief, even though the lack of norms is equally important as the loss of value-optimality.

V. THE EROSION OF PRIVACY IN PUBLIC: LACK OF NORMS

We confine our discussion to a consideration of a single example: Facebook.<sup>115</sup> It collects a massive amount of information from its users through their activities on Facebook as well as other sites. It uses the information to allocate costs and benefits. Facebook uses the information primarily for advertising purposes, so the costs it distributes include the costs of receiving possibly unwanted advertising as well as all the costs of having your information in the hands of another. The benefits that the advertising-supported Facebook allocates consist of all the benefits of using the site plus the benefit of receiving possibly relevant advertising. Facebook does *not* distribute the advertising profiles it creates of its users to third parties; it requires the advertisers to describe the type of customers they wish to reach, and it arranges the delivery of the advertisements. Facebook does, however, serve as a conduit to distribute massive amounts of information. Users distribute the information they post to anyone who is able to search for it, including potential employers and government agencies, and third party apps distribute

---

<sup>115</sup> We consider several other examples in SLOAN AND WARNER, *supra* note 41.

information. A detailed analysis of each of these three aspects of Facebook would certainly be interesting, but it is not necessary here.

A. No Shared Conception of Role Appropriateness

There no relevant shared conception of role-appropriate information processing for Facebook. This is clear from the constant controversy surrounding Facebook's privacy practices.<sup>116</sup> If Facebook and its users shared a conception of the approximate boundaries of permissible data collection, use, and distribution, controversy would be minimal. Instead, Facebook's practices have sparked controversy from the very beginning.

Controversies about privacy characterize lack of norms situations. The root cause is business's enthusiastic embrace of information processing. "The past fifteen years have seen extensive investments in business infrastructure, which have improved the ability to collect data throughout the enterprise. Virtually every aspect of business is now open to data collection and often even instrumented for data collection."<sup>117</sup> Businesses do not invest merely to improve existing business practices, they also invest in novel forms of commercial interaction based on innovative uses of information, Facebook being one of many examples. The innovations typically outrun the relatively slow evolution of social norms and give rise to situations characterized by the lack of any relevant shared conception of role-appropriate information processing, a sure sign of the lack of relevant informational norms.

---

<sup>116</sup> See Chris Burns, FACEBOOK PRIVACY RULES CHANGING: DATA COLLECTION, USE, PERSONALIZED ADS, SLASHGEAR (2013), <http://www.slashgear.com/facebook-privacy-rules-changing-data-collection-use-personalized-ads-29295380/> ("Changes to its privacy policies over the years led to a flood of complaints from consumers concerned over how Facebook handles their personal information." See also Justin Lafferty, INFOGRAPHIC: THE HISTORY OF FACEBOOK'S PRIVACY CHANGES [2013], [http://allfacebook.com/infographic-the-history-of-facebooks-privacy-changes\\_b116292](http://allfacebook.com/infographic-the-history-of-facebooks-privacy-changes_b116292).

<sup>117</sup> PROVOST AND FAWCETT, *supra* note 112 at \_\_\_\_.

B. A Similar Four-Part Pattern

The lack of norms cases exhibit a pattern similar to the loss of value-optimality cases.

(1) *Facebook defends its practices as appropriate.* In December 2009, Facebook changed the default privacy settings from “private” to “everyone,” a setting that made status updates and shared content publicly accessible. Facebook founder Mark Zuckerberg defended the change by claiming that “[p]eople have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.”<sup>118</sup> In a conference call with reporters to explain and defend the change, Facebook’s then CEO, Sheryl Sandberg, sounded the same “evolution” theme: “by talking in sweeping terms about Facebook’s ambitions to lead ‘an evolution from the information Web to the social Web,’ in which the company has ‘made it safe’ for people to ‘have their real identity online.’”<sup>119</sup> Facebook offered a similar “really in users’ interest” defense of its 2011 partnership with Datalogix.<sup>120</sup> To increase the effectiveness of Facebook advertisements, Datalogix correlates users’ responses to the advertisements while on Facebook with their brick-and-mortar purchases.<sup>121</sup> Facebook describes the practice as “win-win”: “Advertising helps keep Facebook free. We believe we can create value for the people who use our services every day by

---

<sup>118</sup> Marshall Kirkpatrick, FACEBOOK’S ZUCKERBERG SAYS THE AGE OF PRIVACY IS OVER, READWRITE (2010), [http://readwrite.com/2010/01/09/facebooks\\_zuckerberg\\_says\\_the\\_age\\_of\\_privacy\\_is\\_ov#awesm=~oua0mtUEGOEJiS](http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov#awesm=~oua0mtUEGOEJiS).

<sup>119</sup> Rob Pegoraro, FASTER FORWARD: AS FACEBOOK PRIVACY SETTINGS CHANGE, COMPANY’S EXECs DEFEND THE CHANGES, THE WASHINGTON POST (2010), [http://voices.washingtonpost.com/fasterforward/2010/04/facebook\\_privacy\\_contd.html](http://voices.washingtonpost.com/fasterforward/2010/04/facebook_privacy_contd.html).

<sup>120</sup> See Zach Rodgers, HIGH ON THE FACEBOOK HOG, DATALOGIX RAISES \$25M, ADEXCHANGER.COM (2013), <http://www.adexchanger.com/data-exchanges/high-on-the-facebook-hog-datalogix-adds-25m-investment/>.

<sup>121</sup> See Brad Smallwood, MAKING DIGITAL BRAND CAMPAIGNS BETTER (2012), <https://www.facebook-studio.com/news/item/making-digital-brand-campaigns-better>.

offering relevant ads that also incorporate industry-leading privacy protections. In our view, this is a win-win situation for marketers and for you.”<sup>122</sup>

Facebook took the same “really in users’ interest” approach to “sponsored stories,” launched in 2011. A “sponsored story” is an advertisement that indicates that a Facebook user “likes” (in the Facebook sense) an advertised item or has “checked-in” (in the Facebook sense) to announce his or her presence on the premises of an advertised business.<sup>123</sup> The effect was to make it appear that the user had actually *endorsed* (“sponsored”) the business or product.

Facebook initially defended sponsored advertisements as a way to serve users’ interests:

Imagine that you are driving down the freeway and you see a billboard for the latest Pirates of the Caribbean movie. Then you notice your friend's face is emblazoned across the billboard as well, with their opinion of the movie, "I thought Johnny Depp was better than ever!" highlighted for you to see! *The creators of the billboard know that YOU would be most interested in seeing your OWN friend's opinion of the film*, not the opinion of a critic or a stranger. So the billboard intuitively showed you the most influential message possible. Sponsored stories are essentially the same thing, on a much smaller scale.<sup>124</sup>

Facebook announced that it will stop its use of sponsored stories in April 2014: “marketers will no longer be able to purchase sponsored stories separately.”<sup>125</sup> Users will still be associated with advertisements, however, because “social context—stories about social actions your friends have taken, such as liking a page or checking in to a restaurant—is now eligible to appear next to all ads shown to friends on Facebook.”<sup>126</sup> The official rationale is “to simplify Facebook ads,

---

<sup>122</sup> Facebook, RELEVANT ADS THAT PROTECT YOUR PRIVACY (2012), <https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125>.

<sup>123</sup> See Understanding Facebook’s Sponsored Stories, FACEBOOK (2011), <https://www.facebook.com/notes/hyperarts-web-design/understanding-facebooks-sponsored-stories/10150320031255844>.

<sup>124</sup> *Id.* (emphasis added).

<sup>125</sup> An Update to Facebook Ads, FACEBOOK (2014), <https://www.facebook.com/notes/facebook-and-privacy/an-update-to-facebook-ads/643198592396693>.

<sup>126</sup> *Id.*

including eliminating different types of ads that had the same purpose and making our ads look more consistent.”<sup>127</sup>

(2) *Consumers object to Facebook’s data collection and use practices.* As we noted earlier, Facebook’s practices have been controversial from the beginning, and remain so.<sup>128</sup>

(3) *They nonetheless continue to conform to Facebook’s data collection.* Privacy concerns have not kept users away from Facebook. Facebook has grown from one million monthly active users in 2004 to 1.5 billion in 2013; it posted its first annual profit of \$35 million in 2009 and has increased dramatically in profitability since then.<sup>129</sup> As one commentator remarked, “Facebook basically knows enough about me to successfully predict what I’m going to wear tomorrow, yet we all grudgingly accept Zuckerberg’s evil empire and go on with our status updates.”<sup>130</sup> Facebook does allow users to adjust their privacy settings, but that option does not provide a viable way for users to avoid going along with Facebook’s data collection and use practices. The settings provide *very little* control over how *Facebook* collects and uses data.<sup>131</sup> Instead, the settings allow users to control access by other Facebook users.

---

<sup>127</sup> *Id.*

<sup>128</sup> Victoria Craig, FACEBOOK PLAYS DEFENSE ON A NEW ROUND OF PRIVACY CONCERNS (2012), <http://www.foxbusiness.com/technology/2012/10/02/facebook-plays-defense-on-privacy-concerns>. As we have argued elsewhere, there is good reason to think Facebook deliberately makes it difficult. UNAUTHORIZED ACCESS, *supra* note 41 at 342 – 344.

<sup>129</sup> See Stephen Heller, FACEBOOK’S INCREDIBLE GROWTH STORY IN 6 CHARTS, THE MOTLEY FOOL (2013), <http://www.fool.com/investing/general/2013/10/12/facebooks-incredible-growth-story-in-6-charts.aspx>; Thorin Klosowski, HOW FACEBOOK USES YOUR DATA TO TARGET ADS, EVEN OFFLINE LIFEHACKER (2013), <http://lifehacker.com/5994380/how-facebook-uses-your-data-to-target-ads-even-offline> (“For most people, Facebook’s advertising system is insider-baseball that doesn’t really affect how we use the service.”).

<sup>130</sup> See, e.g., Wendy Schuchart, GOOGLE PRIVACY POLICY CHANGES? GET OVER IT, CIO SYMMETRY (2012), <http://itknowledgeexchange.techtarget.com/cio/google-privacy-policy-changes-get-over-it/> (“Facebook basically knows enough about me to successfully predict what I’m going to wear tomorrow, yet we all grudgingly accept Zuckerberg’s evil empire and go on with our status updates”).

<sup>131</sup> Facebook allows some control over how advertisements are displayed and over what advertisements get displayed. See Facebook Ads, FACEBOOK (2014), <https://www.facebook.com/settings?tab=ads&view>, and Manage Blocking, FACEBOOK (2014), <https://www.facebook.com/settings?tab=blocking>.

Even that degree of control is difficult to exercise. The controls are notoriously complicated,<sup>132</sup> and only a relatively small percentage of users change their settings from Facebook's default settings, which maximize public access.<sup>133</sup> In addition, changing the settings to reflect your privacy preferences is quite difficult. In a Columbia University experiment, *none* of the 65 participants were able to set their privacy settings in the way they intended.<sup>134</sup> The participants were Columbia University students. If students at a world class university cannot successfully adjust their Facebook settings, who can?

(4) *It is not consistent with their values.* The privacy controversies that show there is no shared conception of role appropriateness also establish that Facebook's privacy practices do not accord with its users' values. This is hardly a surprise. The explanation is the same as in the earlier examples. Users desire more control, control that is essential to realizing a multifaceted self.

### C. What Is To Be Done?

The situation is dire. A pervasive and increasing lack of relevant norms governing novel transactions compounds the privacy-undermining effect of norms that are no longer value-optimal.

---

<sup>132</sup> See App Settings, (2014), <https://www.facebook.com/settings?tab=applications>; Facebook Ads, *supra* note 131; Follower Settings, FACEBOOK (2014), <https://www.facebook.com/settings?tab=followers>; Manage Blocking, *supra* note \_\_\_; Notifications Settings, FACEBOOK (2014), <https://www.facebook.com/settings?tab=notifications>; Privacy Settings and Tools, FACEBOOK (2014), <https://www.facebook.com/settings?tab=privacy>; Security Settings, FACEBOOK (2014), <https://www.facebook.com/settings?tab=security>; There are eight different pages, each with multiple options, options that themselves have multiple options. Timeline and Tagging Settings, FACEBOOK (2014), <https://www.facebook.com/settings?tab=timeline>.

<sup>133</sup> See eMarketer, MOST FACEBOOK USERS DON'T UNDERSTAND PRIVACY SETTINGS EMARKETER (2011), <http://www.emarketer.com/Article.aspx?id=1008729&R=1008729>.

<sup>134</sup> See MICHELLE MADEJSKI, MARITZA JOHNSON & STEVEN M. BELLOVIN, THE FAILURE OF ONLINE SOCIAL NETWORK PRIVACY SETTINGS (2011), <http://www.futureofprivacy.org/wp-content/uploads/2011/07/The%20Failure%20of%20Online%20Social%20Network%20Privacy%20Settings.pdf>.

Ever-emerging technological possibilities and the ingenuity of planners generate a steady stream of new ways of creating, capturing, and using personal data for one institutional purpose or another. And these innovations, planned or accomplished, pose one challenge after another to the privacy-protecting Davids, who mobilize thinly stretched resources against organizational Goliaths. Off the record, privacy defenders confess to worries about the long-term prospects for their cause. The problem, they say, is not that their efforts may fail, though inevitably this is often true. Perhaps more disturbing is the fact that even the most notable victories often appear as provisional non-defeats-subject to rude reversal down the road . . . Then there is the pervasive sense, widely shared among privacy-watchers, that public opinion is growing complaisant or even fatalistic concerning privacy invasion.<sup>135</sup>

What is to be done?

*What Is to Be Done? Burning Questions of Our Movement* was Vladimir Lenin's 1902 call to revolution.<sup>136</sup> We also issue a call to a revolution. It is essential to act now to reverse the erosion of norm-implemented privacy in public by creating value-optimal role-appropriate informational norms and thereby safeguard the realization of multifaceted selves. This is a critical time. If nothing is done, peoples will eventually become habituated to what now appear as privacy invasions. Informational norms will evolve that permit what *now* appear to be massive invasions of privacy, and people will embrace those norms as value-optimal because the process of habituation will have changed their values. Now is the time to reverse this trend. Doing so requires a sound analysis of what has gone wrong, and we hope we have provided that in our analysis of informational norms and so hope for a better outcome than the deplorable outcome Lenin achieved with his seriously flawed analysis. History will judge:

History will record what we, here in the early decades of the information age, did to foster freedom, liberty, and democracy. Did we build information technologies that protected people's freedoms even during times when society tried to subvert them? Or did we build technologies that could easily be modified to watch and control?<sup>137</sup>

---

<sup>135</sup> RULE, *supra* note 1 at 144.

<sup>136</sup> VLADIMIR LENIN, *WHAT IS TO BE DONE? BURNING QUESTIONS OF OUR MOVEMENT*. (1902).

<sup>137</sup> Bruce Schneier, *RISKS OF DATA REUSE CRYPTO-GRAM* (2007), <http://www.schneier.com/crypto-gram-0707.html>.

We have posed norm-generation strategies elsewhere.<sup>138</sup> We conclude by describing a serious hurdle any attempt to generate norm will confront.

## VI. IS IT ALL OVER?

Attempts to create informational norms can face a Tragedy of the Commons situation in which the needed norm is not sustainable. We illustrate the problem with a fictionalized version of the 1884 introduction of the Eastman Kodak “snap camera.” We then consider how to avoid the Tragedy of the Commons.

### A. A Tragedy of the Commons

The snap camera was a startling innovation. Photography was a mid-nineteenth century invention, but, prior to the snap camera, cameras were quite large and required expertise to use. Portraits were expensive and required posing motionlessly for three to six seconds. The snap camera was cheap, portable, and required neither expertise nor pose time. Candid photos became possible, and that created a privacy problem. The "Hartford Courant" sounded the alarm: "the sedate citizen can't indulge in any hilarriousness without the risk of being caught in the act and having his photograph passed around among his Sunday School children."<sup>139</sup> The camera was nonetheless hugely popular (especially at the 1889 World Fair, where their users were called “Kodak fiends”). This is the kind of situation for which coordination-facilitating informational

---

<sup>138</sup> SLOAN AND WARNER, *supra* note 41.

<sup>139</sup> David Lindsay, *THE KODAK CAMERA STARTS A CRAZE*, PBS (2000), <http://www.pbs.org/wgbh/amex/eastman/peoplevents/pande13.html>. *See also* DANIEL J. SOLOVE, *THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET* 107–108 (2007). Solove quotes Robert Ellis Smith: “In the years before the development of photography in the mid-1800s, even mirrors were not universal in British and American home life. Imagine the realization that for the first time the very essence of your being-your visage-could be captured by someone else-used and controlled by someone else.”; ROBERT ELLIS SMITH, *BEN FRANKLIN’S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET* 126 (2000).

norms provide a solution. Photographers need the cooperation of the people they photograph, who must not run away, hide, make (unwanted) faces, or attack the photographer. The people in turn need the photographers' cooperation. Photographers should not take pictures or distribute them in ways that are too invasive of personal lives or too disruptive of the activities photographed. A role-appropriate informational norm would implement a regime of selective disclosure that allowed the taking of some pictures while prohibiting others. A variety of norms corresponding to different roles (private individual, journalist, photographic artist, etc.) would be required.

It would be interesting to study the development of norms governing the taking of candid photos in public, but our purposes are better served at this point by turning to fiction. Our fiction is that, at some point after the introduction of the snap camera, someone—Kodak, a group or privacy advocates, or the government—proposed a role-appropriate informational norm that everyone agreed was value-optimal. We ignore the likely need for a number of norms, and focus on the single proposed norm (which is really just a stand-in for any norm that might develop). Our argument is both conditional and general: *No matter what* norm is proposed and accepted as value-optimal, people will not conform to it. They will not, that is, given one plausible assumption.

The assumption is that those subject to the norm are, in a certain sense, self-interested. In this case, a classic Tragedy of the Commons<sup>140</sup> arises. For those unfamiliar with the Tragedy of the Commons, we sketch out what happens. Consider Phoebe. Phoebe is self-interested in this

---

<sup>140</sup> The tragedy of the commons was first described in Garrett Hardin, *The Tragedy of the Commons*, 162 *SCIENCE* 1243 (1968). Hardin's historical claims and public policy conclusions have drawn sharp criticism. See ELINOR OSTROM, *GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION* (1990). We do not endorse Hardin's historical or policy claims. Our concern is entirely with the structure of the preferences that give rise to the situation Hardin labels the tragedy of the commons, the name that is now standard for that situation.

sense: she prefers that all others conform to the norm while she does not. That way she gets the benefits of the value-optimal tradeoff while still being able to take and share pictures whenever and however she wants. More precisely, Phoebe has the following preferences in the following order. She prefers: (1) not to conform when most do; (2) conform when most conform (so she constrains her picture taking but contributes to the value-optimal tradeoff); (3) not conform when most also do not (she does as she pleases, but so does everyone else, and there is no value-optimal tradeoff); (4) conform when most do not (she constrains her behavior for no gain). What will she do? She will not conform. She will reason this way. "One of two things will happen: most will conform, or most will not. If most conform, then I should not. I get what I most want, and get the benefits of the value-optimal tradeoff. If most do not conform, then I should not. There is no point in my not taking and sharing pictures as I want when not doing so will not contribute realizing the value-optimal tradeoff." If most people are self-interested in the same way, they will all reason in the same way, and it will be impossible to realize the desired norm.

The same reasoning applies when the actor is not an individual but, for example, a profit-motive driven business and the choice is between conforming to a norm and increasing profits by information processing. Suppose the business is self-interested in the sense of having these preferences in this order. It prefers: (1) not to conform when most do (it maximizes profits and gets the benefits of the value-optimal tradeoff); (2) conform when most conform (it gets benefits of the tradeoff while not being constrained in ways others are not); (3) not conform when most also do not (it opts for the profit maximizing strategy but so does every other business, and there is no value-optimal tradeoff); (4) conform when most do not (it would reduce profits without a value-optimal tradeoff). Any business with these preferences will not conform to a proposed value-optimal norm. That does not bode well for the creation of informational norms.

The only way to avoid such Tragedy of the Commons situations is to change the actors' preferences. There are two ways to do this. One is legal regulation that penalizes non-conformity so heavily (with fines, for example) and with such certainty that non-conformity is no longer a profit-maximizing strategy. This may be necessary, but it is an unattractive option. Effectively regulating business behavior in this way is uncertain, difficult, and expensive. An alternative is to change actors' commitments so that the first preference is to *conform* when most others conform. The suggestion is no pipedream. Commitments to ideals can and do make people devote themselves to the welfare of others in ways they never would without the commitments. Examples include public interest lawyers, university professors devoted to teaching, reassuring surgical nurses, helpful strangers, and devoted parents. They might advance their careers more successfully with more attention to profitability and less to their ideals, but it is the commitment to ideals that explains their behavior.

#### B. Values

Values can make people devote themselves to the welfare of others in ways they never would without the commitments. Public interest lawyers, university professors devoted to teaching, reassuring surgical nurses, helpful strangers, and devoted parents might advance their careers more successfully with more attention to profitability and less to their values, but it is the values that explain their behavior. Suppose people value coordinating with others to realize value-optimal privacy tradeoffs, and suppose they value that enough that "conform when others conform" is their first place preference. That is, given a choice between "conform when most others do to realize a value-optimal tradeoff" and "not conform when most others do," they will

choose to conform. They will, that is, as long as, and only as long as, they believe most others will do so as well. Their conformity is conditional on their believing others will conform.

Conformity is conditional upon realizing society-wide privacy tradeoffs because realizing such tradeoffs is like entering elevators. In elevators, there is no point in being a “nearest neighbor distance maximizer” unless most others are. Similarly, since you need the cooperation of others to realize society-wide privacy tradeoffs, there is no point in trying to do so unilaterally. You may still act in a privacy-respecting way even when others do not, but you are not thereby trying to realize a society-wide value-optimal privacy tradeoff. You know that to be impossible. You are just doing what your own values require you to do. The conditional nature of conformity has an importance consequence. It means valuing coordinating with others to realize value-optimal privacy tradeoffs is by itself not enough to ensure the coordination. People also have to trust each other to act in accord with their values.

### C. The Need for Trust

To see why, suppose Phoebe, like everyone else in her society, values coordinating with others to realize value-optimal privacy tradeoffs. Phoebe, however, does not think the others will act in accord with their values. It does not matter why she thinks this, but suppose she has recently had experiences that give her a dim view of human nature (recently betrayed by friends, for example). Now suppose the question before Phoebe is whether she should coordinate with others in a way that will realize a value-optimal privacy tradeoff. Since she will conform because, and only as long as, most others do, she will not conform.

Creating role-appropriate informational norms requires creating both appropriate values and sufficient trust that people will act in accord with those values. But isn't it naïve to think this

is likely? In many cases, the norms are supposed to constrain business information processing, and the constraints will compete with the profit motive. The profit motive plays a central role in market economies. As the noted economist Arthur Okun observes, monetary rewards “provide the incentives for work effort and productive contribution. In their absence, society would thrash about for alternative incentives—some unreliable, like altruism; some perilous, like collective loyalty; some intolerable, like coercion or oppression.”<sup>141</sup> Isn’t it naïve to think that businesses will abide by the constraints? We think not. Profit motive driven businesses operate within a web of trust:

Society can't function without trust, and our complex, interconnected, and global society needs a lot of it. We need to be able to trust the people we interact with directly: as we sit next to them on airplanes, eat the food they serve us in the cabin, and get into their taxis when we land. We need to be able to trust the organizations and institutions that make modern society possible: that the airplanes we fly and the cars we ride in are well-made and well-maintained, that the food we buy is safe and their labels truthful, that the laws in the places we live and the places we travel will be enforced fairly. We need to be able to trust all sorts of technological systems: that the ATM network, the phone system, and the Internet will work wherever we are. We need to be able to trust strangers, singly and in organizations, all over the world all the time. We also need to be able to trust indirectly; we need to trust people we don't already know and systems we don't yet understand. We need to trust trust.<sup>142</sup>

Is it possible to create the values and trust necessary to establish enough informational norms to secure sufficient privacy in public? If not, it really is all over.

The realization of multifaceted selves will be sharply constrained, and we—all of us—will begin to disappear from the scene.

## VII. A WORRIED AFTERTHOUGHT

---

<sup>141</sup> ARTHUR OKUN, *EQUALITY AND EFFICIENCY* 119 (1975).

<sup>142</sup> BRUCE SCHNEIER, *LIARS AND OUTLIERS: ENABLING THE TRUST THAT SOCIETY NEEDS TO THRIVE* 243 (2012).

We originally ended here, but the following question plagued us to the point that we added this afterword. Has society already crossed a tipping point with respect to the use of Google (and Bing, and the other search engines)? What drives our worry is that people do what is easy, available, and rewarding, and Googling is all three. Enter a few words (on the smartphone you carry everywhere<sup>143</sup>) and get informative results. A recent anecdote in *New York* magazine illustrates how much things have changed in just one decade:

Ten years ago, on our first date, a woman looked at me with terror when I told her that I had Googled her and found the designer-shoe company she ran on the side. The look said: *What else do you know?* But sometime in the last decade, the practice of furiously Googling people stopped being creepy and became standard operating procedure.<sup>144</sup>

If this really is “standard operating procedure,” a tragedy of the commons undermines any attempt to establish a Google-restrictive informational norm: your first choice will be to Google others regardless of whether they Google you.

The example concerns individuals, not businesses, but businesses too have access to an immense variety of information services that are easy, available, and rewarding.<sup>145</sup> We worry that an equally immense variety of tragedies of the commons are unfolding with the result that privacy by voluntary restraint—voluntary restraint by *either* individuals *or* businesses—is suffering the same fate as privacy by obscurity: shrinking into insignificance. This afterword is our response. We reiterate our call to reverse the erosion of privacy in public. We hope we are

---

<sup>143</sup> See Aaron Smith, SMARTPHONE OWNERSHIP 2013, PEW INTERNET (2013), <http://www.pewinternet.org/2013/06/05/smartphone-ownership-2013/> (noting that the majority in the US use a smartphone) (last visited Feb 14, 2014).

<sup>144</sup> Graeme Wood, *Scrubbed*, NEW YORK, 2013, <http://nymag.com/news/features/online-reputation-management-2013-6/> (last visited Feb 13, 2014). This article is about the new nearly \$5 billion a year business of online reputation management, which illustrates just how important and universal the process of Googling has become.

<sup>145</sup> The earlier examples are adequate evidence, but for one more revealing instance, see IMS HEALTH HOLDINGS, INC., FORM S-1 REGISTRATION STATEMENT UNDER THE SECURITIES ACT OF 1933 6, 85, 91–93 (2014), [http://www.sec.gov/Archives/edgar/data/1595262/000119312514000659/d628679ds1.htm#rom628679\\_1](http://www.sec.gov/Archives/edgar/data/1595262/000119312514000659/d628679ds1.htm#rom628679_1) (describing wide reach of IMS Health’s information services).

not caught in a tragedy of the commons in which we—we multifaceted selves—turn ourselves into shadows of what we once were. If this is our fate,

The fault . . . is not in our stars,  
But in ourselves, that we are underlings.<sup>146</sup>

---

<sup>146</sup> WILLIAM SHAKESPEARE, *JULIUS CAESAR*, Act 1, Scene 2, lines 140 – 141 (Cassius speaking to Brutus).