2016

I'll See: How Surveillance Undermines Privacy by Eroding Trust

Richard Warner, *Chicago-Kent College of Law*
Robert H. Sloan, *University of Illinois at Chicago*

Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 32 | Issue 2 Article 3

8-12-2016

"I'll See": How Surveillance Undermines Privacy By Eroding Trust

Robert H. Sloan

Richard Warner

"I'LL SEE": HOW SURVEILLANCE UNDERMINES PRIVACY BY ERODING TRUST

Robert H. Sloan[†] and Richard Warner[††]

Neil Richards and Woodrow Hartzog argue persuasively that "modern privacy law is incomplete because from its inception it has failed to account for the importance of trust." We address the open question of how privacy law should "account for the importance of trust." We combine the focus on trust with another theme: the dehumanizing effect of surveillance. As the security expert Bruce Schneier notes, "psychologists, sociologists, philosophers, novelists, and technologists have all written about the effects of constant surveillance. . . . It threatens our very selves as individuals. It's a dehumanizing tactic employed in prisons and detention camps." We address the open question of why (and under what conditions) it does so. The link between the loss of trust and the dehumanizing effects of surveillance not only makes a compelling case that privacy law should preserve trust and prevent dehumanization, but also suggests how it can do so.

TABLE OF CONTENTS

[†] Professor and Head, Department of Computer Science, University of Illinois at Chicago.
[††] Professor of Law, Chicago-Kent College of Law, Visiting Foreign Professor, University of Gdańsk, Poland.

INTRODUCTION

In Shakespeare's *Othello*, Iago manipulates Othello into worrying that his wife, Desdemona, may be unfaithful. In response, Othello declares,

> I'll see before I doubt; when I doubt, prove;
>
> And on the proof, there is no more but this,
>
> —Away at once with love or jealousy![1]

Othello's plan is to suspend judgment until he collects enough data to "see" whether Desdemona is faithful. The irony is that his "I'll see" changes what he sees. Before, Desdemona was his "soul's joy,"[2] and he trusted her to be faithful. His "I'll see" suspends that trust and leads him to brush aside her professions of love as lies. In addition, and importantly for our purposes, the "I'll see" destroys Desdemona's trust in Othello.[3]

---

1. WILLIAM SHAKESPEARE, OTHELLO (Stephen Orgel & Russ Mcdonald eds., 2001), act 3, sc. 3.

2. *Id.* at act 2, sc. 1.

3. *See, e.g.,* Shakespeare, *supra* note 1, act 4, sc. 2, where Desdemona remarks,

Contemporary surveillance has the same "I'll see" plan as Othello. Or, better a *similar* plan. The analogy is far from perfect. Othello both conducts the surveillance *and* interacts with Desdemona as husband and wife. Businesses and governments are nonetheless importantly like Othello: they collect data to see what people are like in order to treat them accordingly.[4] We are concerned with the effects on individuals who, like Desdemona, do not conduct that surveillance themselves.[5] The *Othello* analogy, while imperfect, is still enough on point to sharply pose the question of whether surveillance undermines trust among individuals who live their lives under a pervasive investigative gaze.

The question is as neglected as it is important. As Neil Richards and Woodrow Hartzog persuasively argue, "modern privacy law is incomplete because from its inception it has failed to account for the importance of trust."[6] We combine our consideration of trust with another urgent concern: the threat pervasive surveillance poses to the self. As many have argued, "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."[7]

I have none [no husband]. Do not talk to me, Emilia.

I cannot weep, nor answers have I none

But what should go by water [be expressed in tears].

4. JAMES B. RULE, PRIVACY IN PERIL: HOW WE ARE SACRIFICING A FUNDAMENTAL RIGHT IN EXCHANGE FOR SECURITY AND CONVENIENCE 14 (2007). Rule notes that modern surveillance practices share a distinctive and sociologically crucial quality: "they not only *collect and record* details of personal information; they are also organized to *provide bases for action toward the people concerned*." (emphasis in original) Systematically harvested personal information, in other words, furnishes bases for institutions to determine what treatment to mete out to each individual. *Id.*

5. We note in passing that, in contemporary surveillance, the watcher is indeed also often the watched. As Jeffery Rosen notes, "[t]he sociologist Thomas Mathiesen has contrasted Michel Foucault's Panopticon—a surveillance house in which the few watched the many—with what he calls the "Synopticon" created by modern television, in which the many watch the few. But in the age of the Internet, we are experiencing something that might be called the "Omnipticon," in which the many are watching the many, even though no one knows precisely who is watching or being watched at any given time." JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE 11 (2005). We focus however on business and government surveillance in which the people surveilled are not also conducting the surveillance.

6. Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, ___ STANF. TECH. L. REV. ___ (forthcoming 2017).

7. Michael P. Lynch, PRIVACY AND THE THREAT TO THE SELF THE N.Y. TIMES (June 22, 2013), http://opinionator.blogs.nytimes.com/2013/06/22/privacy-and-the-threat-to-the-self/. *See also* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 127 (2015). The connection between privacy and the self is a standard theme in the privacy literature. *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING

The link among trust, surveillance, and the self is the concept of *privacy in public*.[8] This concept dates back at least to the nineteenth century sociologist Georg Simmel, who observed that people voluntarily limit their knowledge of each other as they interact in a wide variety of roles.[9] Thus, certain information remains private *relative to the interaction* even if it is readily publicly available to others in other contexts. The link to the self lies in the fact that

> [a]t 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.[10]

We argue that adequate self-realization requires adequately "managing relationships between the self and others." That is possible only when people can trust each other to voluntarily limit their knowledge of each other. Surveillance, we contend, erodes trust thereby undermining privacy in public and consequently limiting possibilities for self-realization. This framework allows us to make a compelling case for privacy law to intervene to preserve privacy and protect the self, and it also allows us to suggest *how* the law can do so.

Section I characterizes the ubiquitous "I'll see" of contemporary surveillance. A key point is that the data collected typically fails to adequately represent the values, purposes, and intentions of the

---

PRIVACY 112 (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.").

8. Helen Nissenbaum's work sparked the current focus on privacy in public. See Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. LAW REV. 119 (2004); Helen Nissenbaum, *Toward an Approach to Privacy in Public: The Challenges of Information Technology*, 7 ETHICS BEHAV. 207 (1997); Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW PHILOS. 559–596 (1998). Our approach in terms of norms is indebted to her work. There is a well-established practice in sociology of regarding privacy as existing in public through selective disclosure. *See* Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL LAW REV. 905 (2010).

9. Georg Simmel, *The Sociology of Secrecy and Secret Societies*, 11 AM. J. SOCIOL. 441, 468 (1906).

10. CHRISTENA E. NIPPERT-ENG, ISLANDS OF PRIVACY 22 (2010) (quoting IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL SPACE, TERRITORY, CROWDING 10 (1975).

subjects of that data. We return to this point in Section V when we argue that ubiquitous surveillance undermines trust and poses a threat to the self. The essential background to this claim consists in connections among the concepts of the self, social roles, and privacy in public. We explain those connections in Section II. We argue that people seek to realize a multifaceted self by interacting social roles, and that realizing a social role typically requires a significant degree of control over how one appears to others. Privacy in public consists in significant part in having such control. Section III argues for the following claims. (i) People achieve control over their appearance through conformity to informational norms, which are social norms that govern the collection, use, and distribution of information. (ii) Coordination under informational norms requires not just knowledge, but what game theorists, philosophers, and computer scientists call common knowledge. (iii) Common knowledge underlies an important form of trust. In Section IV, we explain how social roles create common knowledge and hence the relevant kind of trust, and in Section V we explain how the investigative gaze undermines role-based common knowledge and thereby erodes trust. The consequence is an imminent threat of a precipitous decline in opportunities for self-realization. The solution is to appropriately restrict surveillance *while preserving and restoring role-based common knowledge and the trust it creates*. Privacy advocates and policy makers have focused on the first task but ignored the second. We conclude Section V by arguing that the second task urgent. The reason is the threat to the self that pervasive surveillance creates. Section V explains and evaluates that threat.

I. THE INVESTIGATIVE GAZE

Othello's "I see" illustrates what we will call *the investigative gaze*. To investigate is to search out and examine details in order to learn hidden facts. To gaze is to look steadily and intently. Othello looks at Desdemona steadily and intently in hopes of revealing facts that will show whether she is faithful. Businesses and governments gaze steadily and intently virtually everyone searching for facts that will show them what they want to know.

The investigative gaze includes an observational gaze, and a predictive gaze.

A. The Observational Gaze

The "I'll see" of contemporary surveillance gives businesses and governments a massive capacity to observe a person's past. It is that capacity we will refer to as the observational gaze. It is only a small exaggeration to say that the observational gaze records every

> keystroke, each mouse click, every touch of the screen, card swipe, Google search, Amazon purchase, Instagram, "like," tweet, scan—in short, everything we do in our new digital age can be recorded, stored, and monitored. Every routine act on our iPads and tablets, on our laptops, notebooks, and Kindles, office PCs and smartphones, every transaction with our debit card, gym pass, E-ZPass, bus pass, and loyalty cards can be archived, data-mined, and traced back to us.[11]

Data collection is so pervasive that "if you figure that your life is so disorganized, private, and fragmented that no biographer would or could keep track of it, think again—your biography is being written as you read these pages."[12] The information flows into vast databases.

> Retailers, banks, governments, social networking sites, credit reference agencies and telecoms companies, amongst others, hold vast amounts of information about us. They know where we live, what we spend our money on, who our friends and family are, our likes and dislikes, our lifestyles and our opinions. Every year the amount of electronic information about us grows as we increasingly use internet services, social media and smart devices to move more and more of our lives into the online environment.[13]

Not all the stored information is true. Indeed, "databases are riddled with errors and meaningless coincidences."[14] However, while not always true, the observational gaze often is.

---

11. BERNARD E. HARCOURT, EXPOSED: DESIRE AND DISOBEDIENCE IN THE DIGITAL AGE 1 (2015).

12. JOHN GILLIOM & TORIN MONAHAN, SUPERVISION: AN INTRODUCTION TO THE SURVEILLANCE SOCIETY 43 (2012).

13. STEVEN FINLAY, PREDICTIVE ANALYTICS, DATA MINING AND BIG DATA: MYTHS, MISCONCEPTIONS AND METHODS 1 (2014).

14. *See, e.g.*, Simson L. Garfinkel, *Data Fusion: Information of the World, Unite!*, 299 SCI. AM. 82 (2008). A recent study of ratings of creditworthiness from the National Consumer Law Center found that the reports it requested "were riddled with inaccuracies. Errors ranged from the mundane—a wrong e-mail address or incorrect phone number—to seriously flawed. One of the reports combined information about our volunteer with information about two other individuals; other reports listed wrong addresses, relatives, and occupations. Interestingly, eBureau touts its ability to estimate income based on its advanced models and offer insights based upon the consumer's education. Despite that claim, seven of the fifteen consumer reports generated by eBureau contained errors in estimated income, nearly doubling the salary of one

Palantir is a good illustration. Palantir sells "platforms for integrating, managing, and securing data."[15] It can tie "together surveillance video. . . with credit-card transactions, cell-phone call records, e-mails, airplane travel records, and Web search information."[16] To illustrate how their products work, they present a fictional scenario in which Mike Fikri (a fictional character) gets a speeding ticket on his way to Orlando, Florida.[17] The ticket sets off an alert in the CIA's Palantir system, prompting an analyst to search for data. A graphical user interface displays the results: finger print and DNA evidence collected in Cairo; an ATM video from Miami; photos of his rental truck license plate at a tollbooth; phone records showing calls to Syria; and, a map of his national and international movements. Mouse clicks reveal more: Fikri has been wiring money to the people he has been calling in Syria; the Syrians, under investigation already, have been meeting every day for two weeks and have purchased plane tickets with Fikri's money. A map traces the money flow from Cairo to Fikri in Miami, and from Fikri to the Syrians. In light of the information, the Miami police arrest Fikri. Fikri is fictional, but the capacity to know it illustrates is real. The Los Angeles Police Department (LAPD), for example, reports that "Detectives love the type of information it [Palantir] provides. They can now do things that we could not do before. They can now exactly see great information and the links between events and people. It's brought great success to LAPD."[18]

The massive capacity to know evokes the often used metaphor of the Panopticon.[19] The Panopticon is a prison consisting of two

---

participant and halving the salary of another, and eleven of the fifteen reports incorrectly stated the volunteer's education level." PERSIS YU, ET AL., NATIONAL CONSUMER LAW CENTER, BIG DATA, A BIG DISAPPOINTMENT FOR SCORING CONSUMER CREDITWORTHINESS 18 (2014), http://www.nclc.org/issues/big-data.html.

15. About | Palantir, PALANTIR TECHNOLOGIES, http://www.palantir.com/about/ (last visited Jun 14, 2014).

16. Ashlee Vance & Brad Stone, *Palantir, the War on Terror's Secret Weapon*, BUSINESSWEEK (NOV. 22, 2011), http://www.businessweek.com/printer/articles/5771-palantir-the-war-on-terrors-secret-weapon.

17. Fikri is a fictional character Palantir uses when it shows prospective customers how its products work. *See id.*

18. Matt Burns, *Leaked Palantir Doc Reveals Uses, Specific Functions And Key Clients*, TECHCRUNCH (Jan. 30, 2016), http://techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-functions-and-key-clients/.

19. The source of the metaphor is JEREMY BENTHAM, PANOPTICON; OR, THE INSPECTION-HOUSE (2008). As Julie Cohen notes, "[i]mportant work in information privacy often invokes the Panopticon and other visual metaphors to drive home important points about

concentric circular structures. The outermost structure contains the prisoners' cells. The guards occupy the inner most structure, from which they can see into any cell through windows that prevent the prisoners from seeing the guards. The result is that the prisoners never know when the guards are watching. The effect is that the prisoners behave as if they were under constant surveillance. There is little or no "as if" with today's observational gaze. It *actually* watches virtually everyone virtually all the time, and it sees more than just the observable behavior of prisoners confined to cells. It sweeps over vastly more data generated in a wide and diverse range of contexts and provides far more insight into people's inner lives than the Panopticon guards could gain from their occasional observations.

The insight the observational gaze offers is, however, still highly limited and selective. The reason is that data is *acontextual*. "Acontextual" means *not determined by context*, but we will use it in the following special sense. Data is *acontextual* when it does not contain an adequate representation of the context in which it occurred. An adequate representation is one that reveals a relevant range of the values, purposes, and intentions of the subject (or subjects) of that data.

B. Acontextual Data

The following example sets the stage for our discussion of acontextual data.

> A person was doing data entry for a contractor who was developing a tracking system for young people who were under state supervision. The frustration that finally drove her to quit the job was that the architecture of the database didn't allow social service workers to include narrative information about the context of kids' behavior. Simply, the system tracked each student's "success" or "failure" in a number of different programs. So, for example, if students stopped going to an afterschool program because they faced a serious crisis—a death in the family or an apartment fire, for example—a caseworker worker was forced to check a box that reported that they failed to complete the program. Because there was no input box for narrative case notes, there was

information-based risk." JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 124 (2012).

> literally no place in the system to account for the (sometimes pages of) contextual information written in the social workers' reports.[20]

The complaint is that the categories omit contextual information necessary to understand the values, purposes, and intentions that explain *why* the student succeeded or failed. One could, of course, add a checkbox for "death in the family" or "apartment fire," but that would still fail to capture the values, purposes, and intentions behind the student's reaction to those events. One understands values, purposes, and intentions through narratives that integrate them and the context in which they occur into a meaningful pattern. No set of checkboxes, however elaborate, will constitute such a narrative.

The point holds for databases generally. Traditional relational databases[21] store data in tables consisting of rows and columns.[22] Think of each column as labeled on top with some attribute like "height" or "is an iPhone owner." Think of each row as labeled with the name of a person or thing ("John Smith" or "Mazda Miata with license plate so-and-so") or type of person ("Chicago residents" or "Mazda Miatas"). As you go across any row, the entries under the columns indicate the values of attributes, so for example John Smith might be six feet tall and not an iPhone owner.[23] Organizations carefully prepare data before they enter it into their databases.[24] The reason is that

> Data is dirty, filthy, messy stuff. Often it's incorrect, missing or badly formatted, particularly where humans have been involved in creating and/ or collecting it. Sometimes numeric data is held as text, or text data is forced into fixed-length fields resulting in some data being truncated, and so on. Consequently, a lot of the time and

---

20. VIRGINIA EUBANKS, DIGITAL DEAD END: FIGHTING FOR SOCIAL JUSTICE IN THE INFORMATION AGE 95 (2011).

21. *See generally* ABRAHAM SILBERSHATZ, HENRY F. KORTH & S. SUDARSHAN, DATABASE SYSTEM CONCEPTS (6th ed. 2010).

22. A traditional relational database has much the same properties as an Excel spreadsheet, except that its underlying implementation allows it to usefully hold much larger tables, e.g., tables with millions of rows.

23. For an attribute such as "is an iPhone owner" a computer scientist would think of the database entries as indicating one of the two values "true" or "false", but we can equally think of them as indicating that the attribute is present or absent.

24. FINLAY, *supra* note 13 at 95 ("Maintaining data quality has always been an issue with consumer databases. As a consequence, most organizations have checks and controls in place at the points where data enters their systems. Data is only allowed onto their databases once it has been formatted, cleaned, and validated.").

effort. . . can be spent "cleaning" the data before it's ready to be used.[25]

The result is that databases store the formatted and cleaned trails of data detritus people leave behind as they live. They do not store narratives tying events into a meaningful whole that reveals values, purposes, and intentions. The data is, in this sense, highly acontextual. This is no accident. "Institutions—from universities to software companies to public welfare agencies—[are] organized for efficient achievement of their appointed ends."[26] They collect data for their purposes, not to paint faithful narrative portraits of data subjects.

But aren't we overlooking the "big data" revolution? "Big data" consists in large part of *unstructured* data.[27] Examples include multimedia files, "e-mails, blogs, web pages and transcripts of phone conversations."[28] Such data may reveal a person's values, purposes, and intentions—*to some extent*, but it would be a mistake to think it can be worked into "a composite sketch [of the intentions behind] of what we like, whom we love, what we read, how we vote, and where we protest."[29] The "composite sketch" may reveal that Victoria recently read *Sense and Sensibility*, has been married to Victor for thirty years, voted for Obama in 2012, and protested in Chicago against immigration policy.

But it will be much more difficult for it to reveal whether she likes *Sense and Sensibility* (or read it reluctantly for a reading group), Victoria loves Victor (or is staying married for the sake of the children), was an enthusiastic Obama supported (or a disappointed Clinton supporter reluctantly voting for Obama), objects to immigration policy (or is ambivalent and joined the protest to support a friend).

A "composite sketch" will rarely do what a narrative does: integrate context, action, conversation, and soliloquy in a meaningful whole that reveals the values, purposes, and intentions that come to

25. *Id.*

26. RULE, *supra* note 4 at 156.

27. FINLAY, *supra* note 13, at 180 ("These days, things are very different. Organizations are awash with textual and other types of unstructured data. All sorts of customer correspondence, which until the late 1990s would have been held in racks of filing cabinets, is now stored in electronic format; and then there is all that Internet data, such as tweets, blogs and web pages.").

28. *Id.*

29. *See, e.g.*, HARCOURT, *supra* note 11.

fruition in one's observable activity.[30] The "composite sketch" will be an aggregation of diverse sorts of data created in different contexts with a variety of values, purposes, and intentions, but the "sketch" will omit what did not get recorded, and those omissions will include a good part of the relevant context, values, purposes, and intentions.[31]

Acontextual data is not useless—far from it. Palantir illustrates the power of the observational gaze to penetrate into peoples' pasts. Contemporary surveillance does not merely survey the past. It also aspires to predict the future.

C. The Predictive Gaze

"The most prolific use of data mining is to identify relationships in data that give an insight into individual preferences, and most importantly, what someone is likely to do in a given scenario."[32] The government does not, for example, merely observe Fikri's past, it predicts (as the story implies) that he is a terrorist and arrests him.

Businesses and governments use computer-based statistical analysis to make predictions, an approach known as predictive analytics. In many situations, "models created using predictive analytics make better predictions than their human counterparts."[33] This is not particularly high praise. Humans are bad at prediction in the sorts of situations in which the models do better—just *somewhat* better. The predictions are quite often false. Indeed, "most predictive models are quite poor at predicting how someone is going to behave."[34] The results can bemuse:

> I'm able to understand why [the data aggregator] Acxiom thinks I have one child when I have none—I buy gifts for young nieces and nephews. . . Household income is off, and shopping data says that I made one purchase in the last 24 months for online and offline purchases at retailers! That's hysterical! Supposedly I'm interested

---

30. Deborah G. Johnson, et al., *Campaign Disclosure, Privacy and Transparency*, 19 WM. & MARY BILL RTS. J. 959 (2011) (using the metaphor of a house of mirrors to catalogue the ways in which the presentation of information online can create misimpressions and misinterpretations).

31. *See* FINLAY, *supra* note 13 ("Organizations have little control over how [unstructured data is] supplied and formatted").

32. *Id.*

33. *Id.*

34. *Id. See also* JOHN W. FOREMAN, DATA SMART: USING DATA SCIENCE TO TRANSFORM INFORMATION INTO INSIGHT 285 (2013). (noting that "[t]he only guarantee with forecasting is that your forecast is wrong"); Joanna Geary, *DoubleClick (Google): What is it and what does it do?*, THE GUARDIAN, Apr. 23, 2012, http://www.theguardian.com/technology/2012/apr/23/doubleclick-tracking-trackers-cookies-web-monitoring (last visited Dec 18, 2015).

> in cooking, but I hate cooking. Perhaps the one purchase they have me buying in the past 24 months was a cookbook for someone.[35]

The predictive gaze is an often false gaze. That is hardly surprising. The input to the predictions consists of stored data that is to a great extent acontextual,[36] and such data provides a relatively poor basis for predicting behavior. The reason is its limited ability to capture values, purposes, and intentions. By way of illustration, imagine you are trying to predict whether Victoria will remain married to Victor once their children graduate from college in two scenarios. In the first, all you know is that Victoria has been married to Victor for thirty years. In the second, you know that she regards her marriage with Victor as loveless, places a large disvalue on remaining in loveless relationships, and intends to divorce Victor when their children graduate from college. Your knowledge of Victoria's values, purposes, and intentions in the second scenario obviously provides a more reliable basis for predicting what she will do.

Given this limitation, it may seem surprising that in "many organizations across many industries, predictive models are generating useful predictions and are being used to significantly enhance what those organizations are doing."[37] The explanation is that predictive analytics works particularly well as long as the following three conditions are met.

A significant improvement in prediction accuracy, even with low final accuracy. Direct mailing campaigns are a good illustration. If a company mails an offer to a more or less randomly selected list of people with whom it has no prior relationship, about 1% of those contacted respond.[38] Using predictive analytics to select the group to receive the mailing will improve the response rate to 10% to 20%.[39]

Significantly increased benefit from improved prediction accuracy. In the mailing example, the improved response rate can significantly increase sales. The data scientists Foster Provost and Tom Fawcett contend that "the more data-driven a firm is, the more

---

35. Adam Tanner, *Bizarro World Of Hilarious Mistakes Revealed In Long Secret Personal Data Files Just Opened*, FORBES, TECH (Sept. 5, 2013), http://goo.gl/S8BubO.

36. FINLAY, *supra* note 13 (noting that "All of the methods used to create predictive models require data to be well structured, and the data must be categorical (e.g. occupation, marital status and gender) or numeric (e.g. age, income and time at address). A predictive model can't be built if the data is not in one of these two formats.").

37. *Id.*

38. *Id.*

39. *Id.*

productive it is. . . [data driven decision-making] is associated with a 4%– 6% increase in productivity. . . [and] also is correlated with higher return on assets, return on equity, asset utilization, and market value."[40] To yield a *net* benefit, the increased benefit must be greater than the costs it imposes. That is in part a question of the cost of false positives and negatives.

False positives and false negatives either decrease from whatever approach would otherwise be taken or are low in an absolute sense. A false positive is the mistaken indication that the predicted condition is present. A false negative is the mistaken indication that it is absent. In the mailing example, there will be a lot of both. A 10% to 20% response rate is a failure rate of 80% to 90%. So there will be a lot of people mailed who do not respond (the false positives). Inevitably there will also be many people not mailed who would have responded (the false negatives). The costs are relatively low, however. They divide into the costs to the business, costs to consumers, and costs to society as a whole.

Assume consumers who respond ("true positives") are better off. Then, compared to a random list, both business and consumers are better off, since both false positives and false negatives decrease. Compared to not sending direct mail at all, false negatives decrease, but false positives increase. For the business, the cost of false positives is relatively small—the cost of preparing and sending the direct mail. For false positive consumers the cost is simply receiving advertisements to which they do not respond. The costs to society are also low—at least arguably. Indeed, advertising plays a key role in market economies, which require a flow of information between businesses and consumers.

Advertising, and consumer responses to it, is a key component of that flow. It would be interesting to pursue the issues advertising raises, but that lies outside the scope of our concern here. Instead, we continue our examination of the investigative gaze by turning to its use to allocate costs and benefits.

D. Allocating Costs and Benefits

To allocate costs and benefits, businesses and governments use the investigative gaze to construct digital profiles. The profiles are far

40. FOSTER PROVOST & TOM FAWCETT, DATA SCIENCE FOR BUSINESS: WHAT YOU NEED TO KNOW ABOUT DATA MINING AND DATA-ANALYTIC THINKING 6 (2013).

from accurate portraits, as we noted above. Nonetheless, a person's profile is

> constantly touched. It's examined and judged. When we apply for a bank loan, it's our data that determines whether or not we get it. When we try to board an airplane, it's our data that determines how thoroughly we get searched—or whether we get to board at all. If the government wants to investigate us, they're more likely to go through our data than they are to search our homes; for a lot of that data, they don't even need a warrant. Who controls our data controls our lives. It's true. Whoever controls our data can decide whether we can get a bank loan, on an airplane or into a country. Or what sort of discount we get from a merchant, or even how we're treated by customer support.[41]

This pervasive use of profiles means businesses and government use them to allocate costs and benefits in situations in which false positives and negatives impose considerable costs on individuals and society. These costs can be quite high when denying or permitting bank loans, air travel, border crossings, government searches, and preferential treatment. Other examples include employment,[42] health insurance,[43] the extension of credit,[44] direct marketing,[45] price discrimination,[46] and news reporting.[47] In many of those cases it is, to say the least, less than clear that the benefits outweigh the costs.[48]

---

41. Bruce Schneier, *Essays: Our Data, Ourselves*, SCHNEIER ON SECURITY, (May 15, 2008), https://www.schneier.com/essays/archives/2008/05/our_data_ourselves.html.

42. *See* Beth Givens, *Public Records on the Internet: The Privacy Dilemma,* PRIVACY RIGHTS CLEARING HOUSE (April 12, 2002), https://www.privacyrights.org/ar/onlinepubrecs.htm; Joseph Walker, *Do New Job Tests Foster Bias?*, THE WALL ST. J., (September 20, 2012), http://online.wsj.com/article/SB10000872396390443890304578006283936708970.html.

43. *See* ROBERT H. SLOAN & RICHARD WARNER, UNAUTHORIZED ACCESS: THE CRISIS IN ONLINE PRIVACY AND INFORMATION SECURITY 107-09 (2013).

44. *See* RULE, *supra* note 5, at 197-99 (discussing the greatly enhanced ability of creditors to determine whether their criteria of credit worthiness are fulfilled).; Andy Oram, *Credit card company data mining makes us all instances of a type*, O'REILLY RADAR (May 14, 2009), http://radar.oreilly.com/2009/05/credit-card-company-data-minin.html; Charles Duhigg, *What Does Your Credit-Card Company Know About You?*, N. Y. TIMES MAGAZINE, (May 12, 2009), http://www.nytimes.com/2009/05/17/magazine/17credit-t.html.

45. SLOAN & WARNER, *supra* note 43, at 96 (discussing norms involved in direct marketing).

46. 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).

47. 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

It is hardly surprising then that allocative uses of acontextual data have provoked extensive criticism. We briefly review the criticisms, and we contrast them with a second critique. That critique is concerned with the massive capacity to know as realized in the investigative gaze, and it focuses on the effects surveillance has *independently* of its allocative use. We refine and extend this second line of criticism. Before doing so, however, we briefly summarize both critiques in order to set our proposals against the proper background.

E. Two Critiques

We begin with the critique of using the investigative gaze for allocation.

1. The critique of allocation

The critique of using the investigative gaze for allocation takes different forms in the case of the government and private business. The governmental critique focuses on the use of surveillance to discourage and prevent behavior of which the government disapproves.[49] Critics claim that the government *illegitimately* uses surveillance to discourage or prevent activities typically considered permissible in a democratic state.[50] The wide and penetrating reach of governmental surveillance affects a disturbingly long list of types of people.[51] Still, most people are not on that list. So, how does surveillance harm them? Critics answer by identifying a long-term, systemic harm. They contend that some or all of the uses are illegitimate exercises of governmental power that harm society as a whole by limiting free expression and political debate and creating a culture of oppression.[52]

The critique of private business surveillance is diffuse and complex. Our goal, however, is to contrast that critique with the critique of the capacity to know, and for that purpose, it is sufficient

---

reporters can penetrate into people's lives is highly controversial. JON L MILLS, PRIVACY: THE LOST RIGHT 287 (2008).

48. *See, e.g.*, FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015).

49. *See* Robert H. Sloan & Richard Warner, *The Self, the Stasi, and the NSA: Privacy, Knowledge, and Complicity in the Surveillance State*, 17 MINN. J. LAW SCI. & TECHN. 347, 380-84 (2016).

50. *See id.* at 380-81.

51. *See id.* at 380.

52. *See id.* at 372-74 n. 102-16 and accompanying text.

to list six main criticisms. They are that information processing practices: (1) discriminate among individuals in unfair ways,[53] (2) result in a distribution of costs and benefits across society that is unjust,[54] (3) create a chilling effect that leads to excessive conformity,[55] (4) lack transparency and accountability,[56] (5) fail to ensure free and informed consent to the collection and use of data,[57]

---

53. *See, e.g.*, PASQUALE, *supra* note 48, at 72; SLOAN & WARNER, *supra* note 43, at 273-302.

54. *See, e.g.,* DAVID LYON, ELECTRONIC EYE: THE RISE OF SURVEILLANCE SOCIETY 45; RULE, *supra* note 4, at 12.

55. *See, e.g.*, CHRISTIAN PARENTI, THE SOFT CAGE: SURVEILLANCE IN AMERICA FROM SLAVERY TO THE WAR ON TERROR 92 (2004) (noting that "[u]biquitous but fragmented, commercial surveillance helps make us obedient; it create consumers with predictable tastes, borrowers who repay their debts, and personality structures acclimated to cooperation with authority"); HEIDI BOGHOSIAN & LEWIS LAPHAM, SPYING ON DEMOCRACY: GOVERNMENT SURVEILLANCE, CORPORATE POWER AND PUBLIC RESISTANCE 27 (2013) ("Distracted by the rush and convenience of information technology, few of us discern that opening a window into our personal transactions helps shape a culture of conformity and normalizes the nefarious business of domestic intelligence gathering"); PASQUALE, *supra* note 48, at 15 ("In his book Turing's Cathedral, George Dyson quipped that 'Facebook defines who we are, Amazon defines what we want, and Google defines what we think.' We can extend that epigram to include finance, which defines what we have (materially, at least), and reputation, which increasingly defines our opportunities.").

56. *See e.g.*, PASQUALE, *supra* note 48, at 61.

57. The criticism here is extensive. An early and influential critique is Paul Schwartz, *Internet Privacy and the State*, 22 CONN. LAW REV. 815 (2000) (Notice and Choice does not ensure free choice because of information asymmetries, collective action problems, limited rationality, and a lack of market options). More recent critiques include: MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2013) (Notice and choice as implemented is inconsistent with the requirements of free choice); 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 33 (2011), http://www.ftc.gov/os/comments/privacyreportframework/00338-57839.pdf ("Informed consent in the digital marketing era requires . . . a new commitment to candor and honesty .#.#. [the online marketing industry] needs to clearly explain to the user how the data are collected and used"); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DEDALUS 32, 36 (2011) (noting "the transparency paradox. Achieving transparency means conveying information handling practices [however] If notice . . . finely details every [relevant fact] .#.#. we know that it is unlikely to be understood, let alone read. But summarizing practices in the style of, say, nutrition labels is no more helpful because it drains away important details, ones that are likely to make a difference," and arguing for a much greater reliance on context); Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*, *in* PROCEEDINGS OF THE ENGAGING DATA FORUM: THE FIRST INTERNATIONAL FORUM ON THE APPLICATION AND MANAGEMENT OF PERSONAL ELECTRONIC INFORMATION (2009), http://senseable.mit.edu/engagingdata/downloads.html (consumers "confront . . . full-on barriers to achieving meaningful understanding of the practice and uses to which they are expected to be able to consent."); Paul M. Schwartz & Daniel Solove, *Notice and Choice: Implications for Digital Marketing to Youth*, (2009), http://digitalads.org/documents/Schwartz_Solove_Notice_Choice_NPLAN_BMSG_memo.pdf (Notice and Choice fails to ensure a free choice and fails to ensure an informed

and (6) contribute to governmental surveillance in ways that are inadequately regulated.[58]

2. The critique of the capacity to know

The critique of the capacity to know addresses the negative effects surveillance has independently of the allocation of costs and benefits.[59] As Bruce Schneier notes,

> Psychologists, sociologists, philosophers, novelists, and technologists have all written about the effects of constant surveillance, or even just the perception of constant surveillance. Studies show that. . . [s]urveillance strips us of our dignity. It threatens our very selves as individuals. It's a dehumanizing tactic employed in prisons and detention camps around the world.[60]

The open question is why—*and under what conditions*—surveillance "threatens our very selves as individuals." It does not appear to do so in all cases. Consider public health, for example. Public health officials record details of disease and treatment, often in ways that allow personal identification. That information

> has provided the foundation for planning, intervention, and disease prevention and has been critical for epidemiological research into patterns of morbidity and mortality for a wide variety of diseases and conditions. Registries have been essential for tracking individuals and their conditions over time. Surveillance has also

---

choice); Fred Cate, *The Failure of Fair Information Practice Principles*, in THE FAILURE OF FAIR INFORMATION PRACTICE PRINCIPLES 342, 369 (Jane Winn ed., 2006) ("as transposed into contemporary privacy laws and regulations, FIPPS [Fair Information Privacy Practices] have been used to glorify individual choice as if that, and not appropriate privacy protection, were the goal of data protection. While privacy advocates and policymakers cling tenaciously to FIPPS, at least in their rhetoric, the reality is that FIPPS as applied today largely disserve both privacy and other important societal interests."); J. Howard, III Beales & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, UNIV. CHIC. LAW REV. 109–135, 114 (2008) ("The reality that decisions about information sharing are not worth thinking about for the vast majority of consumers contradicts the fundamental premise of the notice approach to privacy."); RULE, *supra* note 4 (privacy advocates pay insufficient attention to how to balance privacy versus competing concerns).

58. *See, e.g.,* Bruce Schneier, *The Public-Private Surveillance Partnership*, SCHNEIER ON SECURITY (July 31, 2013), https://www.schneier.com/essay-436.html.

59. *See e.g*., Bruce Schneier, *The Internet is a surveillance state*, CNN (March 16, 2013), http://www.cnn.com/2013/03/16/opinion/schneier-internet-surveillance/index.html; Sandra Fulton, *Senate Report Opens a Window Into Hidden World of Data Aggregators*, AMERICAN CIVIL LIBERTIES UNION, (Dec. 18, 2013), https://www.aclu.org/blog/technology-and-liberty/senate-report-opens-window-hidden-world-data-aggregators; PASQUALE, *supra* note 48, at 61.

60. BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 127 (2015).

> served to trigger the imposition of public health control measures, such as contact tracing, mandatory treatment, and quarantine.[61]

Controversies abound over the appropriate type and acceptable extent of public health surveillance,[62] but few would deny that *some* surveillance is justified, and it seems difficult to see how appropriately circumscribed public health surveillance poses a threat to the self.[63]

We take the critics' concern, however, to be, not with particular cases, but with the consequences of a ubiquity to the investigative gaze and in particular its use to create "profiles of individuals and groups based on their activities, connections, performances, transactions and movements that relate to, among other things, government departments."[64] The concern is that "[o]ur identity is understood by others—and by inanimate machines—more from our data-image than from our personal communication."[65] The problem is that

> [p]articular forms of communication are a vital aspect of what it means to be human. What we disclose to whom, and under what conditions, is highly significant. What once we might have revealed, consciously, about ourselves to someone we trust—friend, doctor, priest, therapist—may now be involuntarily disclosed by electronic means to organizations or machines that we cannot know, let alone trust, in the same way.[66]

The question, however, remains: *why* is pervasive use of digital profiles a threat to identity? There is no question that the ubiquity of the investigative gaze signals a profound change in the way people relate to businesses, governments, and each other, but why isn't that just a *change*? Why is it a "threat to our very selves"?[67]

---

61. AMY L. FAIRCHILD ET AL., SEARCHING EYES: PRIVACY, THE STATE, AND DISEASE SURVEILLANCE IN AMERICA 204 (2007). For concern about the sharing of health information, see, e.g., Lori Andrews et al., *Privacy Policies of Android Diabetes Apps and Sharing of Health Information*, 315 JAMA: THE JOURNAL OF THE AMERICAN MEDICAL ASSOCIATION 1051 (2016), and Lori Andrews, *Ethical, Legal, and Social Issues in Genetic Testing for Complex Genetic Diseases*, VALPARAISO UNIVERSITY LAW REVIEW 793 (2003).

62. *See generally* FAIRCHILD ET AL., *supra* note 61.

63. *Id.*

64. DAVID LYON, SURVEILLANCE AFTER SNOWDEN 81 (2015).

65. LYON, *supra* note 54, at 19.

66. *Id.*

67. BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 127 (2015).

Commentators offer a variety of metaphors that suggest directions in which to pursue possible explanations. People become "mere algorithm fodder,"[68] "nodes of information production,"[69] and puppets manipulated through "invisible threads."[70] Jean Baudrillard offers one of the more elaborate and suggestive characterizations:

> We are constantly confronted with the anticipated statistical verification of our behavior, and absorbed by this permanent refraction of our least movements, we are no longer confronted with our own will. We are no longer even alienated. . . each individual is forced despite himself or herself into the undivided coherency of statistics. There is in this a positive absorption into the transparency of computers, which is something worse than alienation.[71]

We will return to these metpahors in Section V, but our initial guiding metaphor is different. It is *Othello*.

Othello's "I'll see" leads him, under Iago's spell, to construct a "data profile" of Desdemona that paints her as unfaithful, a "whore" in Othello's eyes.[72] Othello constructs the profile out of acontextual

---

68. PASQUALE, *supra* note 48, at 198.

69. RONALD J. DEIBERT, BLACK CODE: INSIDE THE BATTLE FOR CYBERSPACE 63 (2011) (noting 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").

70. ALEKSANDR SOLZHENITSYN, CANCER WARD 208 (2003). The full quote is:

"As every man goes through life he fills in a number of forms for the record, each containing a number of questions . . . . There are thus hundreds of little threads radiating from every man, millions of threads in all . . . they are not visible . . . but every man is constantly aware of their existence . . . . Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads." Bruce Schneier has applied the passage to contemporary surveillance. Bruce Schneier, *The Value of Privacy,* WASH. NOTE, (June 9, 2006), http://washingtonnote.com/bruce_schneier_1/.

71. JEAN BAUDRILLARD, JEAN BAUDRILLARD: SELECTED WRITINGS 213 (2001).

72. *See* SHAKESPEARE, *supra* note 1, [a]ct 4, sc. 2

(DESDEMONA

Alas, what ignorant sin have I committed?

OTHELLO

Was this fair paper, this most goodly book,

Made to write "whore" upon? What committed!

Committed!—O thou public commoner!

I should make very forges of my cheeks,

That would to cinders burn up modesty,

Did I but speak thy deeds.—What committed!

Heaven stops the nose at it, and the moon winks;

The bawdy wind, that kisses all it meets,

Is hush'd within the hollow mine of earth,

data—data torn out of the context that reveals values, purposes, and intentions. A good example is Othello's eavesdropping s on a conversation between Iago and Cassio about Cassio's mistress, Bianca. Iago sets up both the conversation and the eavesdropping because he knows that Othello will interpret the conversation to be about Cassio's non-existent affair with Desdemona, and

> As he [Cassio] shall smile Othello shall go mad;
>
> And his unbookish jealousy must construe
>
> Poor Cassio's smiles, gestures, and light behavior
>
> Quite in the wrong.[73]

Othello does "go mad." He no longer trusts Desdemona and summarily dismisses as lies her professions of love. Fixated on her data profile, he no longer perceives the real Desdemona, whom he finally kills—thinking he is killing the data-profile-Desdemona. *Othello* suggests that fixation on acontextual data profiles can destroy trust and threaten the self by rendering it no longer visible. We develop this suggestion in Section V. The essential background consists in important connections among the concepts of the self, social roles, and privacy in public.

II. SELF, SOCIAL ROLES, AND PRIVACY IN PUBLIC

We begin with a summary of the connections we will describe. There are four key points. (1) People typically strive to realize a multifaceted self. (2) One realizes such a self in large part through a variety of social roles. (3) In a wide range of cases, realizing a social role requires a significant degree of control over how one appears to others. (4) Adequate control over how one appears is essential to an adequate degree of privacy in public.

A. The Multifaceted Self

William James characterizes the relevant notion of the self.[74] "I am," James writes,

---

And will not hear it.—What committed!—

Impudent strumpet!).

73. SHAKESPEARE, *supra* note 1, act 4, sc. 1.

74. 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); COLIN MCGINN, THE CHARACTER OF MIND: AN INTRODUCTION TO THE PHILOSOPHY OF MIND 111f. (2nd ed. 1997). For a commitment based theory of the self, *see*

> 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.[75]

James' point is that you make yourself who you are by what you "stand by," that is, by the commitments you freely strive to realize. We take that to be a widely shared conception of the self. One correction is called for, however. James suggests that a *single* commitment defines who you are.[76] On the contrary, the self you seek to realize is a multifaceted self. As John Gray notes, "the 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."[77] This conception of the self underlies liberal political philosophy from John Stuart Mill[78] to John Rawls[79] and Joseph Raz.[80] We place ourselves in this tradition, and assume that the realization of a multifaceted self is an ideal people strive to realize.

You realize a multifaceted self in large part through social roles.[81] To see why, imagine trying to be a bird-watcher in a society

---

RICHARD WARNER, FREEDOM, ENJOYMENT, AND HAPPINESS: AN ESSAY ON MORAL PSYCHOLOGY (1987).

75. WILLIAM JAMES, 1 THE PRINCIPLES OF PSYCHOLOGY 309 (1890).

76. 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." *Id.* at 295.

77. JOHN GRAY, POST-LIBERALISM: STUDIES IN POLITICAL THOUGHT 262 – 263 (1993).

78. *See generally* JOHN STUART MILL, ON LIBERTY (David Bromwich & George Kateb eds., Yale University Press 2003) (1859).

79. *See generally* JOHN RAWLS, A THEORY OF JUSTICE (1971); JOHN RAWLS, POLITICAL LIBERALISM (1993).

80. *See generally* Joseph Raz, The Morality of Freedom (1986).

81. *Id.* at 311 (emphasizing the importance of social roles—what he calls "social forms"—to the development of the self).

that does not recognize that role. You track birds to look at them,[82] but that does not make you a bird watcher in the sense that a member of the Audubon Society is. To be a bird watcher in that sense is to fulfill a role *society recognizes*, and you can refer to that role to explain your actions to yourself and others. In the imagined society, no such explanation is available. You are just a bird-watching anomaly. Similar remarks hold for an immense variety of examples. You cannot be a lawyer, medical doctor, or racecar driver unless society recognizes the role. Even being a parent, child, lover, or spouse take on different meanings depending on the society in which the relationships are realized.[83]

B. Controlling How One Appears

In the case of many roles, realizing them requires a significant degree of control over how one appears to others. We have discussed a number of examples elsewhere.[84] Two examples are sufficient for our purposes here. Students and teachers provide the first example, and journalists the second.

1. Students and teachers

University students and teachers share a goal that they can realize only if they can control how they appear to each other. The goal is that teachers should assign grades only on the basis of relevant academic work.[85] Accepting this goal and seeking to realize it is part of what constitutes properly realizing the teacher role. To reliably achieve the goal, teachers must minimize bias, and that requires that students have a relevant degree of control over how they appear to their teachers. Students need to appear to teachers primarily in the light of their relevant academic achievements, not in light of extracurricular aspects of their personalities, past academic records, honors, or punishments. To ensure the appropriate appearance,

---

82. *Id.* at 310.

83. *See id.*

84. *See* Richard Warner & Robert H. Sloan, *Self, Privacy, and Power: Is It All Over?*, 17 TUL. J. TECH. INTELL. PROP. 61 (2014); Sloan & Warner, *supra* note 49.

85. *See, e.g.*, *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; *Student Records and Confidentiality*, WISCONSIN DEPARTMENT OF PUBLIC INSTRUCTION (2013), http://dpi.wi.gov/sspw/pupil-services/school-social-work/contents/confidentiality/student-records.

students need the cooperation of other students and teachers. The reason is that how you appear to someone depends on what they know about you (you cannot, for example appear truthful to someone who knows you are lying).

Thus, students and teachers must both voluntarily limit themselves. Teachers must limit what they tell other teachers and the university about the students they know, and students must limit their disclosure of what they know about other students.

2. Journalists

Journalists investigating governmental wrongdoing share a goal: protecting the political independence of the press by protecting the identities of their whistleblowing sources from unwanted disclosures.[86] To realize this goal, journalists must appear to both the government *and* to their sources as "essential checks on government and partners in ensuring a healthy democratic debate,"[87] not as criminals whom the state should prosecute. The point finds ample confirmation in the Obama administration's unprecedented threats and prosecutions of journalists. Human Rights Watch and the American Civil Liberties Union report:

> Journalists expressed concern that, rather than being treated as essential checks on government and partners in ensuring a healthy democratic debate, they may be viewed as suspect for doing their jobs. One prominent journalist summed up what many seemed to be feeling: "I don't want the government to force me to act like a spy. I'm not a spy; I'm a journalist."[88]

The complaint is precisely that journalists appear as criminals not as partners. That appearance has a predictable effect on sources: they are reluctant to work with investigative journalists. As *The New York Times* journalist Philip Shenon remarked, "My goodness, if I were one of my sources, I would never talk to me again, even about stories that really would have been a public service."[89] Journalists

---

86. *See, e.g.*, Commisioner for Human Rights, ETHICAL JOURNALISM AND HUMAN RIGHTS COUNCIL OF EUROPE (2011), https://wcd.coe.int/ViewDoc.jsp?id=1863637#P252_37545.

87. Human Rights Watch, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism* (July 2014), https://www.aclu.org/sites/default/files/assets/dem14-withlibertytomonitorall-07282014.pdf.

88. *Id.*

89. Molly Redden, *Is the "Chilling Effect" Real?*, THE NEW REPUBLIC, 2013, http://www.newrepublic.com/article/113219/doj-seizure-ap-records-raises-question-chilling-effect-real (last visited Feb 1, 2015).

need to cooperate with each other to appear appropriately. Faced with the massive power of the state, no journalist can unilaterally ensure that he or she appears as a partner, not a criminal.[90] That takes a concerted effort of a critical mass of journalists—enough to serve as an effective counterweight to state power. This is not to say that the journalists' concerted efforts are always an effective counterweight. The state must also exercise some restraint in the prosecution of journalists.[91]

Similar remarks hold for a wide variety of social roles. People interacting in those roles share a goal that can only be realized through controlling how they appear, and they cannot achieve that control unilaterally but require the cooperation of others. Acquaintances, colleagues, friends, and family typically share the goal of cordial and harmonious relations. Realizing that goal requires controlling appearances through the selective distribution of information, and ensuring selectivity requires cooperation. It is easy to think of relevant goals for any number of other examples involving selective information flows. 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. The clerk in the wine store cannot ask how many ounces of alcohol you consume a day, but your doctor can. 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 and therapist can ask about both. And so on for lawyers, real estate agents, repair services, taxi drivers, mechanics, and on and on.

People's interactions through social roles weave a complex network over which information flows selectively. We have been emphasizing the role of that network in facilitating self-realization. Now we turn from the connections to the self to the connections to privacy. The role-based interactions through which one selectively discloses information create an important kind of privacy.

---

90. *See e.g.,* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014). We discuss the point at greater length in Sloan and Warner, *supra* note 81.

91. Prior to the Obama administration, "the Justice Department's internal guidelines caution prosecutors against compelling the disclosure of the identity of a reporter's sources." RAHUL SAGAR, SECRETS AND LEAKS: THE DILEMMA OF STATE SECRECY 106 (2013).

C. The Privacy Spectrum

Private and public are "sliding scale" opposites.[92] Think of a spectrum whose endpoints are "completely inaccessible to others" (the maximally private end) and "completely accessible to others" (the maximally public end). We divide the spectrum into four regions. Information that is enclosed occupies a region at the maximally private end. To enclose information is to surround it with a barrier that prevents others' access, either entirely or for all but a select group of family, friends, or associates.[93] Obscure information comprises the next region. Information is obscure when it is difficult to find or understand.[94] Information selectively disclosed in role-based interactions follow in that order, and fully public information occupies the maximally public end. Obscurity and role-based disclosure constitute privacy in public. Both facilitate the limited sharing of information. As Bruce Schneier notes, "Privacy isn't about hiding something. It's about being able to control how we present ourselves to the world. It's about maintaining a public face while at the same time being permitted private thoughts and actions."[95]

While enclosure and obscurity both merit detailed discussion, we focus on role-based disclosure. Role-based interactions facilitate the creation of privacy in public through the parties' coordinating their efforts to ensure the selective disclosure of information. People who coordinate in this way are often strangers. This point will play an important role in what follows, so we conclude this section by explaining the point more fully.

To begin, we note that coordination between strangers is just one example of coordination between people when the only relevant knowledge that they have of each other is that they present themselves as being in certain social roles. You may, for example, have known your auto mechanic for years, but know very little about him relevant to your coordination as customer and service provider except that she presents herself as an auto mechanic (and that her efforts seem to keep your car running). The point is the lack of knowledge *relevant to coordination*. When people interacting in

---

92. NIPPERT-ENG, *supra* note 10, at 4 ("[p]rivacy and publicity . . . are each defined with and by each other along [a] conceptual sliding scale.").

93. *See* Sloan and Warner, *supra* note 49 at 354.

94. *See* Woodrow Hartzog & Frederic D. Stutzman, *The Case for Online Obscurity*, 101 CAL REV 1, 1 (2012).

95. Bruce Schneier, *Crypto-Gram,* SCHNEIER ON SECURITY (Sept. 15, 2015), https://www.schneier.com/crypto-gram/archives/2015/0915.html.

social roles coordinate under informational norms, the knowledge they have that is relevant to that coordination is that they present themselves in certain roles. Such role-based coordination is a constant feature of daily life. As Bruce Schneier notes,

> Just today, a stranger came to my door claiming he was here to unclog a bathroom drain. I let him into my house without verifying his identity, and not only did he repair the drain, he also took off his shoes so he wouldn't track mud on my floors. When he was done, I gave him a piece of paper that asked my bank to give him some money. He accepted it without a second glance. At no point did he attempt to take my possessions, and at no point did I attempt the same of him. In fact, neither of us worried that the other would. . . Also today, I passed several strangers on the street without any of them attacking me. I bought food from a grocery store, not at all concerned that it might be unfit for human consumption. I locked my front door, but didn't spare a moment's worry at how easy it would be for someone to smash my window in. Even people driving cars, large murderous instruments that could crush me like a bug, didn't scare me.[96]

Coordination is of course not confined to those whose only relevant knowledge is social roles. It occurs across an entire spectrum of knowledge. The minimal knowledge end is home to those whose relevant knowledge of each other consists primarily in the fact that they are interacting in certain roles. We focus on the region around the "minimal knowledge" end where, even if the people know each other well in some ways, the knowledge they have relevant to coordination consists primarily of their role presentations. We will refer to people in this region as *coordination-strangers*, and we will shorten that to just "strangers" when the context makes it clear what we mean.

Strangers typically coordinate in selectively disclosing information easily, without explicit thought or negotiation. How does that happen? Through informational norms. Understanding how informational norms do so is the key to understanding how the investigative gaze undermines trust.

III. NORM-ENABLED COORDINATION

Informational norms are social norms that constrain the collection, use, and distribution of information. They

---

96. BRUCE SCHNEIER, LIARS AND OUTLIERS: ENABLING THE TRUST THAT SOCIETY NEEDS TO THRIVE 1 (2012).

> 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 professors, we discuss our own grades; at work, it is appropriate to discuss work-related goals and the details and quality of performance.[97]

How do informational norms explain the coordination that creates privacy in public? We answer in two steps. First, we note that the informational norms that facilitate the coordination essential to privacy in public are instances of a particular type of norm—coordination norms. Second, we note that a special knowledge structure explains how coordination norms facilitate coordination. It is that structure that the investigative gaze undermines.

A. Coordination Norms

Driving on the right is a classic example of a coordination norm. Drivers share a goal. Safety and convenience dictate that they drive on the same side as everyone else. No driver can unilaterally realize that goal. Drivers must cooperate with other drivers to do so. In "drive on the right" countries like the United States, drivers realize the goal of driving on the same side by all driving on the right—*as long as they know others will do so too*. If everyone knew that everyone would drive on the left, everyone would drive on the left.[98] They think they ought drive on the left because and only as long as other drivers also drive on the left. We define coordination norms by generalizing from this example.

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 goal, he or she ought to conform to the regularity as long as everyone else does.[99] The "ought" calls for a brief comment. Not all thoughts about what one ought to do are

---

97. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. LAW REV. 119, 120 – 121 (2004).

98. *See* H. Peyton Young, 10 J. ECON. PERSPECT. 105, 107-08 (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).

99. *See* SLOAN & WARNER, *supra* note 43, at 56-59.

effective in generating action. One may think one ought to learn Spanish, but never do it because other demands take precedence. In the case of coordination norms, however, the thought "I ought to conform" typically leads to conformity. Of course, it yields conformity only when people know (or strongly enough believe) that others will conform.

In what follows, we will use "know" as short for "know (or strongly enough believe)." The point to emphasize here is that people think they ought to conform *as long as others do*. So, knowledge is required. People must know that others will (limited exceptions aside) conform; then, they will (limited exceptions aside) conform themselves. This appeal to knowledge to explain conformity is correct as far as it goes, but it is incomplete. It is not just knowledge that explains coordination, but *common knowledge,* a special knowledge structure we characterize in the next section.

Our focus now is on informational norms that are also coordination norms. Not all informational norms are coordination norms,[100] but the ones that concern us are, and from now on we will use "informational norms" to mean "informational norms that are also coordination norms." The coordination informational norms facilitate creates privacy in public through mutual voluntary restraint. We conclude with two examples.[101]

1. Students and teachers

As we noted earlier, students and teachers share the goal that teachers should assign grades primarily on the basis of relevant academic work. Realizing that goal requires that students and teachers coordinate to ensure the selective disclosure necessary to control over how they appear to each other. They coordinate by conforming to the following informational norm: within reasonable limits, students should disclose and teachers acquire only information relevant to evaluating students in the light of their relevant academic achievements. Conformity is conditional because there is no point to

100. "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 probably adhere to the relevant comment norm even if most others did not.

101. Both examples involve professional relationships, but, as the early examples suggest, the points generalize to a variety of different types of relationships. *See supra* text accompanying n. 94. See also Warner and Sloan, *Self, Privacy, and Power, supra* note 82 (discussing a variety of other examples).

in trying to ensure that other teachers have limited information unless enough other students and teachers also limit their information.

2. Journalists

Journalists share a goal: protecting the political independence of the press by protecting the identities of their whistleblowing sources from unwanted disclosures, and realizing that goal requires they cooperate to ensure control over how they appear to each other. Conformity to the following coordination norm ensures that journalists cooperate appropriately: within broad limits, journalists protect the political independence of the press by not revealing the identities of their whistleblowing sources. If journalists can count on conformity to the norm, they can count on appearing as partners in preserving democracy, not criminals.[102] Conformity is conditional. It takes a critical mass of journalists to serve as an effective counterweight to the power of the state. Without it, conforming to the norm does little to protect the independence of the press.

B. What Coordination Requires

In the last section, we provisionally explained norm-enabled coordination by noting that adherents to a coordination norm will conform to it if they know others will. That is not, however, a full explanation of norm-enabled coordination. An example is helpful, and, to that end, we return to the norm of driving on the right. That is not an informational norm, but everything we say will be true of such norms. It just happens to be simpler and clearer to use driving on the right as the sample case.

Suppose Victoria and Victor are stopped in their respective cars at a four-way intersection. Victoria is on one cross street; Victor, on the other. Victor signals a left turn, and a moment later he completes his turn into the lane opposite Victoria. That is what Victoria was sure he would do. But why? She and Victor are strangers. The only relevant fact that she knows about him is that he presents himself in the role of a driver, so it is possible, for all she knows, that Victor is from a left-driving country and will get confused and turn into her.[103] Or, enraged at what he sees as the repressive conformity of modern life, he could have decided to flout convention by driving on the left.

---

102. *See* Human Rights Watch, *supra* note 87.

103. Countries that drive on the left include India, Australia, New Zealand, Southern Africa, the Caribbean, the United Kingdom, Ireland, Malta and Cyprus, among others.

Or it could be that he has never driven before in his life, and has no idea that he is supposed to drive on the right. Or. . . with a little imagination, one might sketch any number of scenarios in which Victor drives on the left. Victoria does not give these possibilities a moment's thought. The same is true of Victor in regard to Victoria. Why?

Our provisional explanation is that she knows Victor will drive on the right, and Victor knows she will do so as well. We still owe an explanation of how they know that, but grant for the moment that they do. The problem is that Victoria can know that Victor will drive on the right without Victor realizing that she knows that. Likewise for Victoria not realizing that Victor knows that she will drive on the right.

Focus for the moment on Victor. Imagine that, if someone were to ask him whether Victoria knew that he would drive on the right, he would reply, "I am not sure. She may think that I am from a left-driving country, will get confused and turn into her, or she may think. . ." where the dots are filled in with the possibilities in which Victor drives on the left. The result is that Victor hesitates to begin his left turn. He worries that Victoria may misinterpret his behavior and, for example, begin evasive action by turning into the left lane just as Victor is also turning into it.

Similar remarks hold for Victoria. If someone were to ask her whether Victor knew that she would drive on the right, she would reply, "I am not sure. He may think that I am from a left-driving country, will get confused and turn into him, or he may think. . . ." Like Victor, Victoria hesitates to begin her turn.

Coordination fails because of a lack of second-level knowledge. It helps at this point to add subscripts to "know" to keep track of levels of knowledge. The problem is that Victoria does not know_2 that Victor knows_1 that she will drive on the right, and the same is true of Victor.

So should we add all second-level knowledge requirements to our explanation of coordination? For Victoria and Victor, this would mean requiring that Victoria knows_2 that Victor knows_1 that she will drive on the right, and that Victor knows_2 the same about Victoria. But then the same problem arises for at the third-level of knowledge. Suppose that Victor knows_2 that Victoria knows_1 that Victor will drive on the right, and suppose Victoria knows_2 the same about Victor. But suppose also that Victor does *not* know_3 that Victoria knows_2 that Victor knows_1 she will drive on the right. Instead, he

thinks, "I know$_2$ that Victoria knows$_1$ that I will drive on the right, but she does not realize I know that. She may think I think she is from a left-driving country, will get confused, and drive on the left." Victor hesitates to begin his left turn. The same third-level doubt can arise for Victoria.

In general, consider any knowledge-level *n* at which Victoria knows$_n$ that. . . knows$_1$ that Victor will drive on the right, and Victor knows$_n$ that. . . knows$_1$ that Victoria will drive on the right. With enough ingenuity one can construct examples in which coordination fails because one of them fails to know$_{n+1}$. . . that the other knows$_1$ that he or she will drive on the right.

When driving, no one gives these possibilities any serious consideration. No one thinks about them at all (with the exception of academics thinking about the theory of coordination when driving). Imagine Victor during his driving test explaining to the examiner, "I realized I had the right of way to make a left turn, but I did not turn because I was worried that the driver on the cross street might not continue to drive on the right." That would be ludicrous. Why? Why do drivers who are strangers to each other never think, "There may be something about the other driver that will lead him or her not to drive on the right?" Why is coordination unhesitating, without explicit thought or negation? The question is well known in game theory, as the following example from the game theorist Michael Chwe illustrates:

> Each person might want to take part in an antigovernment protest but only if there are enough total protesters to make arrests and police repression unlikely. People most often "solve" coordination problems by communicating with each other. Simply receiving a message, however, is not enough to make an individual participate. Because each individual wants to participate only if others do, each person must also know that others received a message. For that matter, because each person knows that other people need to be confident that others will participate, each person must know that other people know that other people have received a message, and so forth. In other words, knowledge of the message is not enough; what is also required is knowledge of others' knowledge, knowledge of others' knowledge of others' knowledge, and so on.[104]

104. MICHAEL SUK-YOUNG CHWE, RATIONAL RITUAL: CULTURE, COORDINATION, AND COMMON KNOWLEDGE 3 (2013).

Chwe's solution is the standard one in game theory. The parties have what game theorists, philosophers, and computer scientists call *common knowledge*. People have common knowledge that they will conform if they know they will conform, know they know it, know they know they know it, and so on.

This is the solution we adopt. Parties to coordination norms coordinate without hesitation because they have common knowledge that the other parties will conform. Common knowledge makes the parties transparent to each other in a way that facilitates coordination based on knowledge of what the other parties will do. Everything is out in the open. There is no possibility of misunderstanding, misinterpretation, doubt, or deception at any knowledge level. We claim that the investigative gaze undermines this transparency and thereby makes people opaque to each other in ways that make coordination problematic. We turn to that claim in Section V. A necessary preliminary is to see how relevant common knowledge can arise among strangers. The only relevant fact that strangers know about each other is that they present themselves to each in certain social roles. How can that scant foundation support the rich structure of common knowledge?

IV. COMMON KNOWLEDGE

We answer by first describing a particularly clear case of common knowledge—eye contact. We then use that as a model to explain how role presentations create common knowledge between strangers.

A. Eye Contact

Imagine that Alice sees Bob, an old acquaintance. She stares at him hoping to remember his name before he sees her. Unfortunately, Bob does see her, and Alice realizes that it would be pointless to pretend she did not see him. It is pointless because the following infinite sequence is true.[105]

We use the phrase "they see each other" as short for "Alice sees Bob, and Bob sees Alice:"

---

105. *See, e.g.*, Peter Vanderschraaf & Giacomo Sillari, *Common Knowledge*, *in* THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta ed., Spring 2014 ed. 2014), http://plato.stanford.edu/archives/spr2014/entries/common-knowledge/ (last visited July 1, 2015); KEN BINMORE & ADAM BRANDEBURGER, COMMON KNOWLEDGE AND GAME THEORY (1988), http://deepblue.lib.umich.edu/handle/2027.42/100630; Paul Milgrom, *An axiomatic characterization of common knowledge*, 49 ECONOMETRICA 219 (1981).

First level:

Alice knows$_1$ that they see each other.

Bob knows$_1$ that they see each other.

Second level:

Alice knows$_2$ Bob knows$_1$ that they see each other.

Bob knows$_2$ Alice knows$_1$ that they see each other.

Third level:

Alice knows$_3$ Bob knows$_2$ Alice knows$_1$ they see each other.

Bob knows$_3$ Alice knows$_2$ Bob knows$_1$ they see each other.

.

.

.

How do Alice and Bob take this infinite series of steps? Start with the first level. Alice knows that Bob sees her by reasoning about Bob. She reasons this way: "I see Bob with his eyes directly in line with mine. Bob has normal perceptual abilities, so I can conclude that Bob sees me. Now I see Bob, so I can conclude that we see each other." Bob reasons the same way about Alice, starting from "I see Alice with her eyes directly in line with mine." This gives us the first level:

Alice knows that they see each other.

Bob knows that they see each other.

This explanation may provoke the incredulous response, "No one reasons like that!"—and rightly so. It is extremely unlikely that Alice (to focus on her) reasons in a way that even approximates the reasoning we have attributed to her, and she need not reason at all. She may just think, "We see each other!" We do not, however, intend the reasoning we attribute to Alice to characterize what she in fact does, but what she *could* do. Alice and Bob have the capacity to explicitly reason their way to knowing that they see each other. We characterize that capacity by exhibiting explicitly the reasoning that Alice and Bob could produce.

The capacity to reason about each other explains how Alice and Bob get to the second-level of knowledge. We describe reasoning as if it was explicit, but again the point is the same: to characterize what Alice and Bob could do, not what they actually do. Alice reasons: "At the first level, I started from the fact I saw Bob's eyes lined up with mine, and I reached the conclusion that Bob sees me. If Bob sees me,

he sees *my* eyes lined up with *his*. Bob has normal reasoning capacities, so, at the first level, Bob will have reasoned just as I did from 'Alice's eyes are lined up with mine' to *his* first-level conclusion that we see each other."

For Alice to realize that fact about Bob is for her to reach the second-level conclusion: "I know$_2$ Bob knows$_1$ we see each other." Bob will reason in the same way to his second-level conclusion that he knows$_2$ Alice knows$_1$ they see each other. Thus:

Alice knows$_2$ Bob knows$_1$ they see each other.

Bob knows$_2$ Alice knows$_1$ they see each other.

Alice and Bob get to the rest of the levels the way they get from the first level to the second: by reasoning about their reasoning at the level below. For any level *n*, Alice reasons about Bob's $n - 1$ level reasoning to reach the conclusion that Alice knows$_n$ Bob knows$_{n-1}$. . . that they see each other, and Bob reasons in the same way to reach the conclusion that that Bob knows$_n$ Alice knows$_{n-1}$. . . that they see each other.

As we emphasized earlier, we are not claiming that Alice and Bob actually reason in this way. We are characterizing a *capacity* to generate an infinite sequence of levels of knowledge. The capacity makes eye contact transparent. It means that Alice and Bob are capable of decisively ruling out any possibility of doubt or deception with regard to their seeing each other at any level of knowledge. There is nowhere to hide, either inadvertently or by design. People achieve a similar transparency when they present themselves in social roles.

The point of our discussion of eye contact is to use it as a model of how social roles create common knowledge. To that end, note that the following feature of eye contact explains how it generates common knowledge. In describing this feature, we focus on Alice, but the same comments hold for Bob, and the fact that what we say is true *for both* is the feature in question. The feature: Alice's having her eyes directly in line with Bob's is sufficient for her to know$_1$ that she sees Bob, *and* her having her eyes directly in line with Bob's is sufficient for her to know$_2$ that Bob knows$_1$ that Alice's eyes are directly in line with his. Social roles give rise to common knowledge in the same way.

B. How Social Roles Generate Common Knowledge

So what is the analogue of having eyes directly in line for social roles? An example helps. Imagine that a student, Roger, visits his

professor, Sarah, during her office hours. Roger presents himself in the role of a student; Sarah presents herself in the role of a professor. Their presentations of themselves in those roles is sufficient for Roger to know$_1$ that Sarah will conform to the student/teacher norm, *and* it is sufficient for Roger to know$_2$ that Sarah knows$_1$ that they present themselves to each other in those roles. The same is true for Sarah: the role presentations are sufficient for Sarah to know$_1$ that Roger will conform to the student/teacher norm, *and* it is sufficient for Sarah to know$_2$ that Roger knows$_1$ that the present themselves in the roles.

To explain how this happens, we begin with sports stadium advertising. The game theorist Michal Chwe notes that, during a game in 1996,

> baseball fans at Cleveland's Jacobs Field [looked] up to see an airplane pulling a banner advertising anonymous HIV testing. Obviously the irony here is the airing of such a sensitive issue as AIDS publicly and even festively on a bright sunny day at the ballpark. . . [The underlying purpose is that] I would be more likely to get an HIV test if I knew that doing so was not unusual, but I wouldn't find this out through everyday conversation; at the ballpark, looking up at the plane, however, it is obvious to all that everyone is seeing the same thing.[106]

Thus, for everyone, seeing the sign was sufficient for knowing that anonymous HIV testing was available, *and*—because it was "obvious to all that everyone is seeing the same thing"—seeing the sign was sufficient for each person seeing it to know that everyone saw it, at least everyone who was paying minimal attention to what was happening above the stadium. These two features made it common knowledge among the "paying minimal attention" group that anonymous HIV testing was available.

The resulting common knowledge comes from two factors: (1) Almost everyone knows that the banner is flying over the stadium, and (2) almost everyone knows that almost everyone knows that. (1) and (2) give rise to the infinite sequence of knowledge levels that constitute common knowledge that a banner is flying over the stadium. (1) and (2) make it a simple matter to get to the first two levels of knowledge.[107]

---

106. CHWE, *supra* note 104, at 41.

107. We are following Davd Lewis. "[T]he basic idea behind Lewis' argument is that for a set of agents, if a proposition A is publicly known among them and each agent knows that everyone can draw the same conclusion *p* from A that she can, then *p* is common knowledge." Vanderschraaf & Sillari, *supra* note 105. The same idea underlies Stephen

Suppose, for example, Colin and Megan are sitting together in the stadium. Colin reasons this way at his first level of knowledge. "I know I see the banner, and I know that Megan does too. So we both know that a banner is flying over the stadium." Megan reasons in the same way to *her* first-level conclusion that they both know a banner is flying over the stadium.

At the second level, Colin reasons as follows: "I reasoned to my first-level conclusion from the fact the Megan knows that a banner is flying over the stadium to the conclusion that we both know that. Megan knows that I know that a banner is flying over the stadium, so she will have reasoned in the same way the to *her* first-level conclusion that we both know that a banner is flying over the stadium." For Colin to reach that conclusion is for him to know that they know that a banner is flying over the stadium. Megan reasons in the same way to her conclusion that they both know that they know. Once they get to the second level, Colin and Megan reach the rest of the levels by reasoning about their reasoning at the levels below.

Of course, flying banners over stadiums is not the only way to create situations in which "it is obvious to all that everyone is seeing [learning, apprehending] the same thing."[108] Education and acculturation also routinely provide a basis for common knowledge in the same way.[109] In the United States, for example, a process of explicit and implicit instruction, discussion, and correction makes it obvious to everyone—at least those with a minimum of basic education—that everyone learns that George Washington was the first president of the United States. Thus, not only is it true that: (1) almost everyone in the United States learns that George Washington was the first president; it is also true that (2) almost everyone knows that almost everyone learns that. Social roles and associated informational norms generate common knowledge in this way.

Consider the student/teacher norm. In the appropriate group (which includes at least students and teachers at large universities), education and acculturation result in everyone knowing that students and teachers conform to the student/teacher norm, and in everyone knowing that everyone knows that everyone is subject to that process of education and acculturation. So, not only do students and teachers

---

Schiffer's treatment of common knowledge (which he calls "mutual knowledge"). STEPHEN SCHIFFER, MEANING 32-35 (1973). Following CHWE, *supra* note 104, at 41, we add an account of how a proposition can become "publicly known."

108. CHWE, *supra* note 104, at 41.

109. TALCOTT PARSONS, THE SOCIAL SYSTEM (2012).

know that students and teachers adhere to the student/teacher norm, they know that they know that. The result is common knowledge of conformity to the norm.

Roger and Sarah, for example, get to the first level of knowledge as follows. Roger reasons: "I see us interacting as student and teacher. As a teacher, Sarah adheres to the student/teacher norm, and I know I adhere to that norm, so I conclude that we both conform to the norm." Sarah reasons the same way about Roger to the conclusion that she knows that they both conform. So we have:

Roger knows_1 that they conform to the norm.

Sarah knows_1 that they conform to the norm.

Roger and Sarah get to the second level reasoning about their first level reasoning. Roger reasons: "Sarah knows that I know students and teachers conform to the norm. So, at the first level, she will have reasoned from my knowing that to the conclusion that I know that we conform to the norm." For Roger to reach that conclusion is for him to know_2 that Sarah knows_1 that they conform. Sarah reasons the same way about Roger and thus she know_2 that he knows_1 that they conform. So we have:

Roger knows_2 that Sarah knows_1 that they conform to the norm.

Sarah knows_2 that Roger knows_1 they conform to the norm.

They get to the rest of the levels in the same way, by reasoning about their reasoning at the level below. As in the eye contact example, these attributions of reasoning do not characterize reasoning that Roger and Sarah actually produce. They characterize a *capacity* they share. That capacity makes them transparent to each other as far as coordination under the student/teacher norm is concerned. They are capable of ruling out any relevant possibility of doubt or deception with regard to their conformity under the norm, so, as with eye contact, there is nowhere to hide, either inadvertently or by design.

Their transparency is a form of trust.

C. Trust

Our equation of transparency and trust may seem wrong. After all, isn't it *obvious* that trust *contrasts* with knowledge? Isn't trust a matter of having faith that something is true when you do *not* know that it is? Those points are obvious—on *one* traditional understanding

of trust.[110] There is, however, another tradition that contrasts trust with the lack of a *certain sort* of knowledge, not with the lack of knowledge *per se*. The sociologist Barbara Misztal exemplifies this tradition when she remarks that "[t]rust always involves an element of risk resulting from our inability to monitor others' behaviour, from our inability to have a *complete* knowledge about other people's motivations."[111]

We align ourselves with this second tradition. Our focus is on strangers whose only relevant knowledge of each is that they present themselves to each other in certain social roles. There is always "an element of risk resulting from our inability to monitor others' behavior." A person who appears to fulfill a certain role may not actually adhere to the norms associated with that role.

When Roger enters Sarah's office, she assumes that he belongs to the group students and teachers for whom it obvious that everyone learns that students and teachers conform to the student/teacher norm. She could be mistaken. Perhaps it is Roger's first week at the university after growing up in a small town where his source of information about higher education was his cousin, George. George dropped out in his sophomore year and, embittered by the experience, convinced the credulous Roger that professors secretly pooled their information about students to use it all against them.[112]

To get common knowledge out of role presentations, you have to make background assumptions about the efficacy of processes of education and acculturation. People do routinely make those assumptions, as their thought and action shows. The result is a vision of others as transparent as far as coordination under norms goes. We treat this vision as a form of trust. We define the special notion of trust we will use as follows. You *trust another person to conform to a norm* if, based on the relevant role presentations, it is common knowledge between you that each of you will conform.[113]

Some may still wonder why we bother to talk about trust. Couldn't we just talk about knowledge based on role presentations?

---

110. *See e.g.*, ADAM B. SELIGMAN, THE PROBLEM OF TRUST 21 (2000).

111. BARBARA MISZTAL, TRUST IN MODERN SOCIETIES: THE SEARCH FOR THE BASES OF SOCIAL ORDER 18-19 (1996) (emphasis added).

112. *Id.*

113. There are a wide variety of treatments of trust and coordination. *See, e.g,* ANDREW H. KYDD, TRUST AND MISTRUST IN INTERNATIONAL RELATIONS (3rd ed. 2007); KATHERINE HAWLEY, TRUST: A VERY SHORT INTRODUCTION 4–5 (2012); KAREN COOK, RUSSELL HARDIN & MARGARET LEVI, COOPERATION WITHOUT TRUST? (2007).

We could, but we would lose something essential. We would be overlooking the fact that our daily role-mediated dependencies on others occur within a web of associations and evaluations, a web that has the concept of trust at its center. Talk of trust keeps those association and evaluations at center stage. Talk of trust underscores the remarkable fact that people confidently predict how complete strangers will act based solely on the fact that they present themselves in a certain role. Role-based trust is a constant feature of daily life. As the Nobel Prize winning economist Elinor Ostrom notes,

> As we go about our everyday life, we interact in a wide diversity of complex situations. Many of us face a morning and evening commute where we expect that others, who are traveling at great speeds, will observe the rules of the road. Our very lives depend on these expectations. Others depend on our own driving behavior conforming in general to locally enforced rules about speeding, changing lanes, and turn-taking behavior at intersections. Those of us who work in large organizations—universities, research centers, business firms, government offices—participate in a variety of team efforts. In order to do our own work well, we are dependent on others to do their work creatively, energetically, and predictably, and vice versa.[114]

Trust of strangers in the form of common-knowledge-created transparency is a pervasive feature of daily life. The investigative gaze undermines this trust.

It does so by undermining the common knowledge on which trust (in our sense) depends. Role presentations serve as a basis for common knowledge in part because they provide a basis for knowing that others will conform to norms. As we argue it the next section, the investigative gaze subverts the ability of role presentation to generate the first-level knowledge that others will conform to norms. Without first-level knowledge, there is no reasoning to replicate to yield knowledge at higher levels. The consequence is that role-based common knowledge disappears. The transparency of common-knowledge-based trust vanishes along with it, and people become opaque to each other.

V. THE LOSS OF TRUST AND THE THREAT TO THE SELF

We explain how the investigative gaze undermines the capacity of role presentations to serve as a basis for knowing that others will

114. ELINOR OSTROM, UNDERSTANDING INSTITUTIONAL DIVERSITY 4 (2005).

conform, and we then consider the consequences for norm-enabled coordination. To fully evaluate those consequences, we turn to the threat the investigative gaze poses to the self.

A. How Surveillance Undermines Trust

An example is helpful in explaining how the investigative gaze undermines the capacity of role presentations to serve as a basis for knowing that others will conform. Imagine Edward, a whistleblowing source with classified government information, contacts Glenn, a well-known investigative journalist. Glen assumes the government will turn its investigative gaze on his interactions with the source, and that other investigative journalists are, and believe they are, under surveillance. Those assumptions are correct,[115] but their truth does not matter for the purposes of the example. What matters is the effect of journalists' believing they are true. Specifically, is presenting yourself as a journalist still sufficient for other journalists to know that you would conform to the journalist norm given the power of today's governmental investigative gaze?

Perhaps not. The point of conforming to the norm is to ensure a politically independent press by refusing to disclose the identity of sources. The investigative gaze makes it extremely difficult to conceal the identity of a source even if a journalist refuses to disclose it, so the point of refusing to disclose disappears.

In addition, surveillance can readily give the government evidence of a journalist's communications with a source and of a journalist's receiving and concealing classified or sensitive information. The consequences may include government harassment, imprisonment for refusal to disclose a source, and, in national security cases, prosecution under the Espionage Act.[116]

Against this background, Glen asks, "Will other journalists, most of whom are strangers to me, conform to the journalist norm? Can I predict based merely on their presentation of themselves as journalists that they will conform?" How can he confidently answer yes? Previously, a journalist's role presentation was a reliable predictor of conformity when refusing to disclose a source's identity effectively concealed the source's identity. But it no longer is now when the government can easily focus its gaze on activities that were formerly

115. *See generally* GREENWALD, *supra* note 90; SAGAR, *supra* note 91. We discuss the issues at some length in Sloan & Warner, *supra* note 49.

116. *See* SAGAR, *supra* note 91, at 105, 154.

easy to conceal. Different people will act differently. Some may conform to express their allegiance to the ideal of a politically independent press. Some may conform because "that is what journalists do," or for various other reasons. Others will not conform on the ground that doing so has lost its point and incurs increased risks.

For people he knows well, Glen may be able to assign some rough probability to his prediction of what they will do, but, in the case of strangers, Glen will not have enough information to do that. All he will know is that different people will react differently, and he will be unable to assign any even rough probability to whether they will conform or not. We will describe these cases as instances of *uncertainty*.[117]

This pattern repeats itself for other norms. In general, the main reason for conforming to informational norms is the selective control of the flow of information. The investigative gaze reduces, if it does not eliminate, the point of conforming by reducing, if not eliminating, the parties' ability to conceal a wide range of information.[118] In addition, being under the investigative gaze carries with it unpredictable consequences, and, in a wide range of cases, increases the risk of unwanted consequences, both known and unknown.

Assume—for the moment—that people are aware of the reach and power of the investigative gaze. Then, different people will react differently, and in the case of strangers, one will not have enough information to assign any even rough probability to whether they will conform. One will be uncertain. It follows that, among strangers, role presentations are no longer sufficient for people to know that others will conform to norms. Common knowledge collapses, trust vanishes, and people become opaque.

Grant, for the moment, that the loss of trust leads to a decline in coordination under informational norms. That would entail a decline

---

117. This technical use of "uncertainty" is standard in economics. *See* KEN BINMORE, RATIONAL DECISIONS 35 (2011); OSTROM, *supra* note 114, at 49.

118. For a similar view, see Margot Kaminski, *Regulating Real-World Surveillance*, 9 WASH. LAW REV. 1113 (2015); Margot Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 UNIV. RICHMOND LAW REV. 456 (2015). *See also* Leysia Palen & Paul Dourish, *Unpacking "Privacy" for a Networked World*, *in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 129–136 (2003), http://doi.acm.org/10.1145/642611.642635; Valerian J. Derlega & Alan L. Chaikin, *Privacy and Self-Disclosure in Social Relationships*, 33 J. SOC. ISSUES 102–115 (1977); VALERIAN J. DERLEGA & ALAN L. CHAIKIN, SHARING INTIMACY: WHAT WE REVEAL TO OTHERS AND WHY (1975).

in privacy in public, because privacy in public arises in significant part from coordination under informational norms. The decline in privacy in public carries with it a decline in the ability to realize the wide range of social roles that require a significant degree of privacy in public. Opportunities for self-realization wane significantly, and people lead impoverished lives compared to those they can still lead now.

Fortunately, at present, in a wide range of cases, people continue to coordinate under informational norms. Their coordination facilitates the privacy in public people need to realize social roles that depend on restricted flows of information. So our assumption that norm-enabled coordination declines may be wrong. One may also question our assumption that people know and understand the investigative gaze.

Our point is that both assumptions are likely to become true in the near future. So, the threat of a serious loss of opportunities for self-realization, while it remains just a *threat*, is nonetheless an imminent one. Even if people do not understand the reach and power of the investigative gaze today, they are increasingly aware of surveillance and its effects.[119] So turn the clock forward to the time when people are well aware of the investigative gaze. Once they are, role-based-common knowledge among strangers disappears, and strangers become opaque as the transparency of common-knowledge-based trust vanishes. Will coordination under informational norms decline?

Perhaps but not necessarily. The loss of common knowledge leaves people uncertain about whether others will conform, and what people do when they are uncertain depends on how they value the relevant outcomes.[120] If they value conformity enough, they will still conform.

---

119. *See* PEW Research Center for the People & the Press July 2013 Political Survey, PEW RESEARCH CENTER FOR PEOPLE & THE PRESS (2013), http://www.people-press.org/files/legacy-questionnaires/7-26-13 NSA Topline for Release.pdf (Post-Snowden, knowledge of government surveillance is widespread. According to a 2013 PEW survey, "50% of Americans answered 'a lot' to 'How much, if anything, have you heard about the government collecting information about telephone calls, e-mails and other online communications as part of efforts to monitor terrorist activity?' Another 37% answered 'a little.' Totaling the percentages yields 87% with some knowledge of government surveillance and hence—possibly—some knowledge of their own complicity.).

120. We offer a game-theoretic model in support of this claim in Sloan & Warner, *supra* note 49, at 393-402; Robert H Sloan & Richard Warner, *The Harm in Merely Knowing: Privacy, Complicity, Surveillance, and the Self*, 19 J. INTERNET LAW 3 (2015).

Consider a non-norm example first. Suppose that Victor prefers to attend the opera if Victoria attends as well, and prefers to stay home alone if she does not. He is uncertain whether she will attend. Whether Victor will go to the opera depends on how much he values the options relative to each other. If he values going to the opera highly enough, he will go even though he is uncertain whether she will. Conformity under informational norms is the same. A person will conform even in the glare of the investigative gaze if the person values the consequences of conformity sufficiently more than the consequences of non-conformity. So, if enough people value conformity highly enough, people may continue to coordinate under informational norms. The observable behavior will look the same as it does when common-knowledge-based trust leads parties to coordinate. What is going on, however, is very different. Trust allows strangers to coordinate *knowing* the other will. When people are uncertain whether others will conform, their conformity is the placing of a bet on an outcome to which they can assign no particular probability.

We think this is a plausible explanation of the current pattern of conformity to informational norms in the presence of the investigative gaze. As increasing awareness of surveillance undermines common knowledge, people will conform as long as they place a sufficiently high value on the coordination that results when both they and others conform.[121] "Sufficiently high" is be high enough to make conformity a more attractive choice than non-conformity. In the journalist and source example this corresponds to the attitude, "The conformity of the community of journalists is so important to me that I will conform on the chance that others will conform."[122]

In either case, if such conformity to informational norms in the presence of the modern investigative gaze persists for long enough, it is plausible people would eventually become accustomed to

---

121. Some may object that many people have not thought enough about surveillance and its consequences to be described as *valuing* conformity under surveillance more than non-conformity under surveillance. Surely many, if not most, people use their smart phone, post on Facebook, and the like without thinking anything like, "Given surveillance, I still value the outcomes of norm-conformity more than non-conformity." Our notion of valuing, however, extends to the cases in which one would explicitly rank conformity higher in value than non-conformity if, under suitably ideal conditions, one were to explicitly consider what one valued.

122. People will also conform if they value what they get from *their own* conformity (no matter what others do) more than the outcomes that flow from non-conformity. In the journalist and source example, this would be the attitude, "I believe so strongly in the 'journalists don't disclose the identity of sources' norm that I'm going to follow it regardless of both surveillance and other journalists' behavior."

effectively revealing a variety of different sorts of information to the investigative gaze and accept doing so as *consistent* with the selective disclosure required by various social roles. Role presentations would again become a reliable predictor of conformity to informational norms even in the presence of the investigative gaze, common knowledge would return and would bring with it the transparency of common-knowledge-based trust. The danger is that people will be too tolerant of the investigative gaze and embrace a world in which ubiquitous and penetrating surveillance both severely restricts opportunities for self-realization and imposes the undesirable political and social consequences outlined earlier.

One countermeasure is obvious: restrict the reach and power of the investigative gaze. Privacy advocates and policy makers have repeatedly recommended and pursued that strategy. There is, however, a second and equally important countermeasure they have ignored: preserve and restore role-based common knowledge. Without it, strangers will remain opaque and opportunities for self-realization will remain limited.

The task is more urgent than it may seem. The amount of time available to carry out the task depends in part on how long norm-enabled coordination continues under conditions of uncertainty. Under such conditions, coordinating is placing a bet on an outcome to which one can assign no particular probability. Coordination will continue as long as people value conformity sufficiently more than non-conformity. The instant peoples' values change coordination collapses. Will people's values change?

That is not unlikely. The investigative gaze creates a threat to the self, and that threat may lead people to assign a large disvalue to the consequences of conformity. If enough people assign a large enough disvalue, people will value non-conformity over conformity, and conformity to informational norms cease. Interaction among people would not cease, of course. It would still be true that "[a]s we go about our everyday life, we interact in a wide diversity of complex situations,"[123] but, without coordination under informational norms, the character of those interactions would profoundly change. One possibility is a world in which an

> implicit bargain. . . is offered to citizens: pose no challenge and you have nothing to worry about. Mind your own business, and support or at least tolerate what we do, and you'll be fine. Put

123. OSTROM, *supra* note 114, at 4.

> differently, you must refrain from provoking the authority that wields surveillance powers if you wish to be deemed free of wrongdoing. This is a deal that invites passivity, obedience, and conformity. The safest course, the way to ensure being "left alone," is to remain quiet, unthreatening, and compliant.[124]

We conclude by examining the threat to the self and considering how likely it is that it will undermine coordination under informational norms.

B. The Threat to the Self

Othello stands as a warning of the potential threat to the self in the "I see" of the investigative gaze. Othello's "I'll see" results in a "data profile" of Desdemona that wrongly represents her as unfaithful. Desdemona's protestations of faithfulness are unavailing. They would have been effective at the beginning of the play when Desdemona's presentation of herself as a loving spouse prompted Othello to call her his "soul's joy," but Othello's "I see" destroys his trust in that role presentation, and, in a display of the destructive power of the combination of loss of trust and acontextual representations, he kills Desdemona and then himself.

The trust-undermining investigative gaze subjects people to a similar misinterpretation through the use of acontextual data. The ubiquity of the investigative gaze entails a loss of control over how you appear, and the heavy reliance on acontextual data means the way you appear to others does not accurately reflect the way you are. That inaccurate representation nonetheless determines to a great extent the risk and benefits that come your way. You contribute to this misrepresentation whenever you conform to informational norms. Conformity has always entailed selectively revealing information. Today, however, even selectively revealing information entails revealing that information to the ubiquitous investigative gaze.

Will people come to place a high enough disvalue on constantly playing into their own misrepresentation that it outweighs the value they place on conformity to informational norms? The metaphors we considered earlier suggest they should, even if they do not.[125] They

---

124. GREENWALD, *supra* note 90, at 195. We discuss possible futures in Sloan& Warner, *supra* note 49, at 403-08.

125. For additional considerations, *see* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2001) (emphasizing the undesirability of acontextual characterizations of people). ONORA O'NEILL, A QUESTION OF TRUST: THE BBC REITH LECTURES 64 (2002) (emphasizing the need to trust "with good judgment").

suggest that pervasive surveillance dehumanizes people. They become "mere algorithm fodder,"[126] "nodes of information production,"[127] and puppets manipulated through "invisible threads."[128] They are "forced. . . into the undivided coherency of statistics. . . [into] a positive absorption into the transparency of computers, which is something worse than alienation."[129]

The metaphors raise questions. Will people see the pervasive presence of the investigative gaze as dehumanizing? Will they as a result assign a high disvalue to exposing themselves through norm-enabled coordination to the distorting use of acontextual data? And will that disvalue be great enough to outweigh the value they place on conformity to norms?

The fact that people still routinely conform to informational norms shows that currently the answer to the second question at least is "No." The answers to both questions *could* change to a clear "Yes," but it seems unlikely that the change would occur for *all* informational norms.

The reason is that different consequences are associated with conformity to different types of norms. Conforming to the journalist norm can expose you to government harassment and prosecution. Compare this with the student/teacher norm in an institution that uses one of the increasingly popular student tracking programs like Jenzabar.[130] Jenzabar offers "a 360 degree view of each student—from academic performance and extracurricular engagement to financial aid and demographic information—providing you with deep insights into potential risk factors and probabilities of success."[131] The risk for a conforming students is that they will be represented (or misrepresented) in ways inconsistent with choices they have made about how to pursue their self-realization. The risk, while serious, is not as grave as prosecution for failure to disclose a source or the possession and use of classified information.

---

126. PASQUALE, *supra* note 48, at 198.

127. DEIBERT, *supra* note 69.

128. SOLZHENITSYN, *supra* note 70.

129. BAUDRILLARD, *supra* note 71, at 210. Alienation, a sense of separation from others, requires a sense oneself as separate and autonomous. Peoples' "absorption" into their digital profiles denies them even that bittersweet solace.

130. JENZABAR, http://www.jenzabar.com (last visited April 5, 2016).

131. *Jenzabar Retention*, JENZABAR (2013), http://www.jenzabar.com/wp-content/uploads/2015/11/Jenzabar_Retention_Brochure_web_2.pdf.

CONCLUSION

In general, the degree of disvalue people assign to conformity under norms will vary as the severity of the risks of conformity vary, and those risks will vary with the type of norm. The result is that the negative effect of people's perception of increased disvalue on coordination spreads across a spectrum from "extreme disvalue" to "minimal disvalue."

The more people's responses gravitate toward the "extreme disvalue" end, the more norm-enabled coordination collapses. This is more than just an abstract possibility. There are a number of examples arguably moving toward the "extreme disvalue" end. The journalist norm and the student/teacher norm are cases in point, as we have argued elsewhere.[132] Other examples include norms involved in hiring and retention, health insurance, the extension of credit, direct marketing, price discrimination, and news reporting.[133]

The solution is to preserve and restore role-based common knowledge. That task has not been on the radar of either public policy makers or privacy advocates, but it very much should be.

---

132. Warner and Sloan, *supra* note 84; Sloan and Warner, *supra* note 49.

133. *See supra* notes 42-47 and accompanying text.

* * *

* * *

* * *