The Chronicle Review

Naked in the 'Nonopticon'

Surveillance and marketing combine to strip away our privacy

By SIVA VAIDHYANATHAN

In November, Facebook, the social-networking site most popular among university students and faculty members, discovered just how much its users care about privacy. Sneaking in a surprise for its roughly 60 million users, it placed little notes about some of their Web purchases in the personal "newsfeeds" on friends' profiles. Through this new "social-advertising" program, Beacon, Facebook ruined quite a few surprise gifts.

But it got a bigger surprise for itself: a user rebellion. Within days of the release of Beacon, more than 70,000 Facebook members signed up for a group on the site protesting the service and the decision to deny users the chance to opt out. The furor reverberated as major news media picked up the story.

In 2006 — when Facebook had released the "newsfeed," through which members receive updates about friends' activities, romantic status, and interests — there had been a small protest as well. But within weeks, Facebook allowed users to turn off the service if they wished, and protest died.

Facebook executives mistakenly assumed that their members were not the sort who cared very much about personal privacy. After all, users readily posted photos from wild parties, lists of their favorite bands and books, and frank comments on others' profiles. Weren't young people some sort of new species used to living "out there," immersed in the details of celebrity lives via PerezHilton.com and Gawker.com, and obsessed with the eccentricities of reality-show contestants? Last year the cultural journalist Emily Nussbaum, writing in New York magazine, had stitched together anecdotes about young people who had no qualms about baring their body parts and secrets on LiveJournal or YouTube.

"Younger people, one could point out, are the only ones for whom it seems to have sunk in that the idea of a truly private life is already an illusion," Nussbaum wrote. "Every street in New York has a surveillance camera," she said. "Each time you swipe your debit card at Duane Reade or use your MetroCard, that transaction is tracked. Your employer owns your e-mails. The NSA owns your phone calls. Your life is being lived in public whether you choose to acknowledge it or not."

True, despite warnings from nervous academics and almost weekly stories about extensive data leaks from Visa or AOL, we keep searching on Google, buying from Amazon, clicking through user agreements and privacy policies (which rarely, if ever, actually protect privacy), and voting for leaders who gladly empower the government to spy on us.

But wait. If young people don't care about privacy, why do they care whether Facebook airs their purchases to hundreds of acquaintances?

It turns out that broad assumptions about the irrelevance of privacy among the young — or the old — share a basic misunderstanding of the issue. That's partly because we too often assume that the word "privacy" stands in for a set of aspects or qualities that people generally wish to keep to themselves: i.e., matters of sex, drugs, and, occasionally, rock 'n' roll.

Privacy is not a clear and common set of traits that might include sexual orientation or HIV status. Nor is it the same issue in every context in which we live and move. "Privacy" is an unfortunate term because it carries no sense of its own customizability and contingency.

When we complain about infringements of privacy, what we really demand is some measure of control over our reputation in the world. Who should have the power to collect, cross-reference, publicize, or share information about us, regardless of what that information might be? If I choose to declare my romantic status or sexual orientation on Facebook, then at least it's my choice, not

Facebook's.

Through a combination of weak policies, vapid public discussions, and some remarkable technologies like camera phones and the Internet, we have less and less control over our reputations every day. (Now we hear that undergraduate researchers at my university have found that a new program for Facebook allows anyone — including an identity thief — to mine our personal pages for data.) And it's clear that people are being harmed by actions that follow from widespread behavioral profiling, whether it's done by the Transportation Security Administration through its no-fly list or Capital One Bank through its high-fee credit cards for those with poor credit scores.

F. Scott Fitzgerald's enigmatic Jay Gatsby could not exist today. The digital ghost of Jay Gatz would follow him everywhere. There are no second chances in the digital age. Rehabilitation demands substantial autonomy and control over one's record — or at least forgiveness. As long as we are held highly accountable for youthful indiscretions that are easily Googled by potential employers or U.S. customs agents, we limit social, intellectual, and actual mobility. And we deny everyone second chances. That's just plain un-American.

Because we have such a poor understanding of what we mean by privacy, and because it so often seems futile to put up a stand against mass surveillance, we must generate better terms, models, metaphors, and strategies to control our personal information. Each of us learns early on that there are public matters and private matters, and that we manage information differently inside our own home and outside it. Yet that distinction fails to capture the true complexity of the privacy tangle.

We each have at least four major "privacy interfaces," or domains, through which we negotiate what is known about us. Each of these offers varying levels of control and surveillance.

The first is what I call person-to-peer. While young we develop the skills necessary to negotiate what our friends and families know of our predilections, preferences, and histories. If we grow up gay in a homophobic family, we learn to cope and exert as much control over such knowledge as we can. If we smoke marijuana in our teenage bedrooms, we learn to hide the evidence. If we cheat on our partners, we practice lying. Those are all privacy strategies for the most personal spheres. Sometimes they work, sometimes not. But the choice rests with us. We feel betrayed when those close to us violate our confidence, and we exact social punishment in accordance with the gravity of the betrayal.

The second is person-to-firm, the flow of information to companies from and about consumers. In this interface, we decide whether we wish to answer the checkout person at Babies "R" Us when she asks for our home phone number. We gladly accept when we are offered what we think are "free" services, like discount cards at supermarkets and bookstores that actually operate as record-keeping account tokens. The clerk at the store hardly ever explains how the system works or what the nature of the transaction really is. We don't always realize what we are giving away when we thoughtlessly reveal a simple piece of data like a phone number or ZIP code. Later, when that fact is matched to our larger profile — an aggregation of thousands of inputs by hundreds of companies — data-analysis companies like ChoicePoint can sell our profile to retailers and service providers. But that accumulation is so far beyond our line of sight that we rarely consider its power and effect.

The third is the most important because the stakes of misuse and abuse are so high: person-to-state. Through census data, tax forms, driver's-license records, and myriad other bureaucratic collections, the state has cause to record traces of our movements and activities. Because the state has a monopoly on legitimate violence, imprisonment, and deportation, the cost of being falsely caught in a dragnet is worth considering no matter how unlikely it seems to be.

The fourth "privacy interface" is poorly understood today and only recently even noticeable (although Nathaniel Hawthorne explained it well in The Scarlet Letter). It's what I call person-to-public: the ways we regulate what those around us know or assume about us. We learn through incidents of shame and embarrassment that strangers can cause harm if they misunderstand us (or sometimes if they understand us too well). So my wife might roll her eyes when I grab an air microphone and pretend I can sing like Frank Sinatra, but I would never act like the Chairman of the Board on my front porch. The person-to-public interface is the subject of a brilliant recent book by the law professor Daniel J. Solove, of George Washington University.

In The Future of Reputation: Gossip, Rumor, and Privacy on the Internet (Yale University Press, 2007), Solove relates the sad story of the "Star Wars Kid." In November 2002, an awkward and pudgy Canadian teenager used a school camera to record himself acting like a character from Star Wars, wielding a golf-ball retriever as a light saber. Some months later, some students at his school discovered the recording, and one posted it on an open file-sharing network. Within days the image of a geeky teenager playing Star Wars became the hit of the Internet.

Millions of people downloaded the video. Soon many of them used their computers to enhance it, adding costumes, special effects, even opponents for the young man to slay. Hundreds of versions still haunt the Web. Many Web sites posted nasty comments about the teenager's weight and appearance. Soon his name and high school became public knowledge. By the time YouTube debuted in 2005, the Star Wars Kid was a miserable and unwilling star of what media activists and analysts like to call "user-generated culture." The real-world harassment drove the kid's family to move to a new town. He had to quit school. The very nature of software, computers, the Internet, and Google made it impossible for the young man to erase the record of one afternoon of harmless fantasy. But the technology was not at fault, Solove reminds us. It was our willingness to shame others and our ease at appealing to free-speech principles that justified such alarming behavior.

No one made any money from that or the other events that Solove offers in his new book. The problem of humiliation occurs outside the familiar political or commercial spheres. In another notable case, Solove describes the "dog-poop girl," a young woman in South Korea who refused to pick up after her dog when riding the subway. Justifiably berated by those who shared the car with her and her dog, the woman found her life turned upside down after being publicly and globally shamed by one of those passengers, who posted photos of the incident on the Web. Solove asserts that while the woman certainly deserved criticism, and even traditional measures of local shaming, to enforce the reasonable norm of cleaning up after one's dog, the level of vitriol and harassment that she suffered was unreasonable and disproportionate to the crime.

What is it about the ease of public surveillance (by, in addition to of, the public) that makes such shaming common and easy? Because of strong traditions of free speech in many developed countries, the state is agnostic on such incidents (although the parents of the Star Wars Kid did receive a $350,000 award for damages after suing the family of the child who posted the video). And although YouTube and Flickr profit from playing host to such occurrences, we can't blame market forces for this phenomenon. Nor are any of these cases security-motivated overreactions. Solove argues our ease with public humiliation for the undeserving (and occasionally the deserving) should trouble us deeply. Like Hester Prynne in The Scarlet Letter, any one of us could find ourselves unable to escape or avoid the marks of our mistakes. We are no longer in control of our public personae as so many of our fellow citizens carry with them instruments of surveillance and exposure.

Solove's book is an honest and troubling account of the ways that we have become our own enemies. But it is short on social analysis. He sees our current predicament as a set of legal problems to be solved. As such, Solove's book serves as a valuable introduction, but hardly a conclusive or comprehensive examination of privacy in the digital era. This emerging issue deserves further examination by social scientists and media scholars.

As an examination of legal and policy intervention, The Future of Reputation is at its best. Solove eschews easy answers and clearly outlines the costs and benefits of potential policies. His most insightful suggestion is that traditional privacy law has distinguished between things that happen in the private sphere and quasi-public areas such as trains, gyms, and malls. That binary is unhelpful in an age in which any one of us might be carrying a video recorder in our pockets and seem all too willing to expose our neighbors. Solove wants the law to move beyond the simple public-private distinction and allow people to seek damages for the exposure of acts that occur outside the home. In addition, he wants the law to punish egregious abrogations of confidentiality within a wide variety of relationships.

A fan of the richness of Internet creativity and its potential to contribute to democratic culture, Solove treads lightly around any idea that might stifle experimentation. But those of us who celebrate our cultural mash-up moment would be delinquent and irresponsible if we ignored the real harms that Solove exposes here.

In an earlier book, The Digital Person: Technology and Privacy in the Information Age (New York University Press, 2004), Solove set the standard for explaining what is at stake in online-data collection and analysis. He walked us through the construction of "digital dossiers" in the second (person-to-firm) and third (person-to-state) interfaces, and outlined the potentials for abuse. That book, like the newer one, explained the limits of law in the pursuit of personal control of information.

The Digital Person was significant because it came out long enough after September 11, 2001, to take into account the U.S. government's notorious "Total Information Awareness" program and other efforts at behavioral profiling. It supplemented the best previous book of social and media theory applied to widespread digital-data collection and private-sector surveillance, the communications scholar Oscar H. Gandy Jr.'s The Panoptic Sort: A Political Economy of Personal Information (Westview Press, 1993).

But 2004 was a long time ago in matters of government surveillance. Solove could not have predicted the revelation in 2005 that the National Security Agency was monitoring American phone calls through a secret program that relied on the cooperation of the major telecommunication companies.

So we are fortunate to have a useful and updated tour through the relationship between the person-to-firm and person-to-state interfaces by James B. Rule, a sociologist at the State University of New York at Stony Brook.

Rule, in Privacy in Peril (Oxford University Press, 2007), strongly makes one point that is either muted or absent in most other solid books about privacy and surveillance: Data collected by one institution are easily transferred, mined, used, and abused by another. So companies like ChoicePoint buy our supermarket and bookstore shopping records and sell them to direct-mail marketers, political parties, and even the federal government. They also collect state records like voter registration, deeds, car titles, and liens to sell consumer profiles to direct-marketing firms. As a result of all that cross-referencing of so many data points, ChoicePoint knows me better than my parents do — which explains why the catalogs that arrive at my home better reflect my tastes than do the ties my father gives me each birthday.

Each data point, each consumer choice, says something about you. If you purchase a few prepaid cellphones and a whole lot of hummus, you might be profiled as someone the Federal Bureau of Investigation should keep an eye on. If you use your American Express Platinum card to buy a latte from Starbucks the day that you purchase a new biography of Alexander Hamilton from Barnes & Noble in an affluent Atlanta ZIP code, you just might be a Republican.

The privacy laws of the 1970s — for which Rule can claim some credit after the critical reception of his 1974 book Private Lives and Public Surveillance: Social Control in the Computer Age (Schocken Books) — sought to guarantee some measure of openness in state data retention. We were to be able to know what the federal government knew about us and thus be able to correct errors. And there were to be strong limits on how government agencies shared such data.

As Rule explains in Privacy in Peril, such common-sense guidelines eroded almost as soon as they became law, largely because the Ford administration, under the influence of a White House chief of staff named Richard V. Cheney, sought to preserve executive power in the face of post-Watergate reforms. In recent years, under pressure from the great enemy of public transparency and accountability, Vice President Cheney, the reforms have been pushed off the public agenda altogether. It's as if Watergate, the Church Committee reports, and revelations of FBI infiltration of antiwar protesters never happened.

That deep historical context sets Rule's work above most other privacy books. Rule writes with a tone of sadness, acknowledging lost opportunities. His understanding of the failure of law matches Solove's. Yet he concludes his book with a call for a reigniting of public-interest movements for better laws that would limit data sharing and demand openness.

Mass surveillance has been a fact of life since the 18th century, Rule argues. This digital moment exposes the extent of it and should rally us to action. But there is nothing new about the bureaucratic imperative to record and manipulate data about citizens and consumers. Digital tools just make it easier. Every incentive in a market economy pushes companies to collect more and

better data on us. Every incentive in a state bureaucracy encourages extensive surveillance. Only widespread political action can put a stop to it. Small changes, like better privacy policies by companies like Google and Amazon.com, are not going to make much difference in the long run, Rule argues. The challenge is too large and the risks too great.

That is a rare and valuable insight. Too often when we consider technology policy and state abuses of power, we restrict our political imaginations. We foolishly consider "corporate responsibility" statements to have real meaning. Or we rely on personal technology like encryption or proxy servers to mask our communications, not recognizing that hiding our own behavior from surveillance does nothing to help our neighbors or improve society. Such "self help" merely ratchets up the arms race of surveillance. Rule demands that we actively change the policies and actions of the state for the greater good. It is refreshing to read a wise and reasoned call for real political action.

Throughout their new books, Solove and Rule both avoid describing mass surveillance as a "Panopticon." That too is refreshing, as that standard model and theory of surveillance has exhausted its utility.

Conceived of as a theory of social control by the 20th century's Michel Foucault, the Panopticon was originally the design of the 19th century's Jeremy Bentham for a prison in which all the inmates would force themselves to behave because they would assume that every moment and act was being observed. Foucault argued that state programs to monitor and record our comings and goings create imaginary cages that limit what citizens do out of fear of being observed by those in power. The mere gaze works as well as an iron cage to control the behavior of most people, the theory goes.

Those who write about privacy and surveillance usually can't help but invoke the Panopticon to argue that the great harm in mass surveillance is social control. However, there are two reasons to doubt the efficacy of the Panopticon as a tool for social control and the relevance of the Panopticon as a model to describe our problems with privacy.

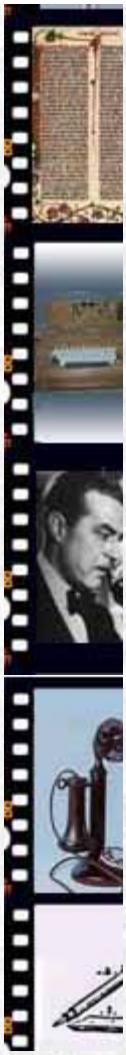
First, people tend to act out and get weird regardless of the number of cameras pointed at them. There are thousands of surveillance cameras in London and New York, yet those cities do not lack for the eccentric and avant-garde. Long before closed-circuit cameras, cities were places to be seen, not to be not seen. Today reality television might indicate that there is a positive relationship between the number of cameras and observers pointed at subjects and their willingness to act strangely and relinquish all pretensions of dignity. There is no empirical reason to believe that awareness of surveillance limits the imagination or cows the creative in a market economy under a nontotalitarian state.

Certainly the Stasi in East Germany exploited the controlling power generated from public knowledge of constant surveillance and the potential for brutal punishment for thought crimes. But that is not our environment in the United States. Basically, the Panopticon must be visible and ubiquitous, or it cannot influence behavior as Bentham and Foucault assumed it would.

Second, what we have at work in America today is the opposite of a Panopticon: what has been called a "Nonopticon" (for lack of a better word). The Nonopticon describes a state of being watched without knowing it, or at least the extent of it. The most pervasive surveillance does not reveal itself or remains completely clandestine (barring leaks to The New York Times). We don't know all the ways we are being recorded or profiled. We are not supposed to understand that we are the product of marketers as much as we are the market. And we are not supposed to consider the extent to which the state tracks our behavior and considers us all suspects in crimes yet to be imagined, let alone committed.

In fact, companies like ChoicePoint, Facebook, Google, and Amazon.com want us to relax and be ourselves. They have an interest in exploiting niches that our consumer choices generate. They are devoted to tracking our eccentricities because they understand that the ways we set ourselves apart from the mass are the things about which we are most passionate. Our passions, predilections, fancies, and fetishes are what we are likely to spend our surplus cash on.

Almost everybody kind of likes Fleetwood Mac's 1977 Rumours. So the fact that I bought the album long ago says nothing special about me. But I am one of the few people who really digs the



bluesy 1969 Fleetwood Mac album Then Play On. That says something about me that might be useful to marketers. It's all about what Wired's editor in chief, Chris Anderson, describes in his book The Long Tail: Why the Future of Business Is Selling Less of More (Hyperion, 2006): market segmentation.

Even the state wants us to be ourselves. It wants subversive and potentially dangerous people to reveal themselves through their habits and social connections, not slink away in the dark to avoid obvious surveillance. After all, the Stasi lost in its efforts to control the East German people, despite exacting long-lasting damage to both the observers and the observed. Our state does not want social or cultural conformity. Domination does not demand it. The state wants to ferret out and punish the ne'er-do-wells and hooligans among us and limit due process along the way. So for the sake of a decent society, we must expose, understand, and confront the Nonopticon.

The insightful books discussed here are a necessary yet insufficient step toward a greater public understanding of the invisible world we have allowed others to build around us. Such systems of surveillance — both commercial and state-sponsored — play a central role in our lives. Yet there are few ways to learn about their pervasiveness and even fewer ways to appeal the effect of their excuses and errors.

We must demand to know the terms of surveillance by our state and its partners in the private sector. We must be allowed to be agents in the construction of our reputations. We must insist on fairness, openness, and accountability in those institutions that commit such widespread surveillance. Otherwise we will cease being citizens. We will be subjects, mere fodder for our watchers, means instead of ends.4

Siva Vaidhyanathan is an associate professor of media studies and law at the University of Virginia. His next book, The Googlization of Everything (googlizationofeverything.com), will be published by the University of California Press in 2009.

http://chronicle.com
Section: The Chronicle Review
Volume 54, Issue 23, Page B7