Harvard Business Review

www.hbr.org

HBR AT LARGE

Privacy as we knew it is virtually gone. Why should you care? What should your business do about it?

What Was Privacy?

by Lew McCreary

Reprint R0810J

Privacy as we knew it is virtually gone. Why should you care? What should your business do about it?

HBR AT LARGE

What Was Privacy?

by Lew McCreary

As best he can, Logan Roots safeguards his privacy by living off the information grid. In a short article in *CSO* magazine (which serves an audience of top security executives), Roots defined privacy as "the freedom to selectively reveal one's self." He described going to great lengths to preserve that freedom by actively frustrating the mechanisms that collect those spores of fact most of us routinely release about ourselves.

"I pay in cash and use false names for as many goods and services as possible," Roots told *CSO* in 2003. "I'm even in a local pool of people who swap [grocery store] club cards....For the past few months I've been using the card of a person who died two years ago. I'm almost sad it's time to switch cards again. I love the dead thing so much."

Most answers to the question "What is privacy?" begin with the individual (usually a living one). Privacy is partly a form of self-possession—custody of the facts of one's life, from strings of digits to tastes and preferences. Matters of personal health and finance, everyone agrees, are in most instances nobody's business but our own—unless we decide otherwise. This version of privacy considers everything we know about ourselves and wish to control but that the continuous capture of our digital existence—the Google searches, the e-mail traffic, the commercial transactions, the cookie-tracked footprints of treks through cyberspace—makes increasingly uncontrollable. All of this behavioral cast-off is the raw material for a granular understanding of what we want or need (whether we know it or not), what we will or won't put up with, and what we might buy or undertake to do—now and in the future.

Today's highly efficient data-gathering and -disseminating mechanisms provoke another, rueful question: "What *was* privacy?" The answer may be that people could once feel confident that what others might find out about them would be treated with reasonable care and consideration, and thus would probably do them no harm. They can no longer. Moreover, the frictionless ease with which government records can now be found online means that reckless-driving citations and SEC violations are accessible to just about anyone.

The face-off between information privacy and information exploitation is a storm ever in the making. Judicial remedies are unlikely to produce a satisfying or sensible balance between companies' economic prerogatives and customers' privacy interest. New technologies—too heedlessly adopted or opportunistically applied—will continue to threaten personal privacy. Business will have to find ways to address this uneasiness. If companies remain complacent, underestimating the degree to which privacy matters to customers, harsh regulation may be waiting in the wings. The best way out is for businesses and customers to negotiate directly over where to draw the lines.

The Shaming of "Dog Poop Girl"

In times past, information flowed fairly inefficiently to a manageably small circle of people. No longer. Daniel J. Solove, an expert in privacy law and an associate professor at George Washington University Law School, begins his 2007 book, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, with an anecdote about a woman in South Korea whose little dog pooped on a subway train. When fellow passengers demanded that she clean up the mess, she told them to mind their own business. One of them took pictures of her and posted them online. She was identified from the pictures, and her life and past were investigated. Eventually she became known throughout cyberspace as "dog poop girl." Solove writes, "Across the Internet, people made posters with the girl's photograph, fusing her picture with a variety of other images. The dog poop girl story quickly migrated to the mainstream media, becoming national news in South Korea. As a result of her public shaming and embarrassment, the dog poop girl dropped out of her university."

Solove's book goes on to chronicle issues of law, civility, and technological capability that are raised by this very modern tale. Among them is the question of whether any act that occurs in a public space strips the parties involved of a right to expect privacy. Solove argues for developing a new definition of privacy to account for the possibility that behavior by someone like dog poop girl can be spread beyond those immediately affected to reach millions of people worldwide. "The Internet," Solove writes, "is indeed a cruel historian. Who wants to go through life forever known as the dog poop girl?"

The intersection of private lives and public spaces brings to the fore a second version of privacy: that it is a feature of the social contract—one that every culture has negotiated for itself over time in order to preserve dignity, civility, and cohesion. In small towns or close-knit social circles, everyone may know quite a lot about everyone else, but all tacitly agree to pretend not to know certain things to which unusual sensitivity attaches.

The two views of privacy come together in David Weinberger, a fellow at the Berkman Center for Internet & Society at Harvard. Weinberger understands people's wish to control their personal information—"Politically, I'm in favor of it"—but he thinks that's only one piece of privacy, and a reductive one at that. "I don't like to talk about privacy that way," he says, "because it seems to reduce the public and the private to a matter of what information we give out."

Instead, he believes, something more basic is at work: "Namely, that we are fundamentally social creatures—insofar as we're creatures who talk and interact. We're inconceivable *not* being social." Thus norms around privacy dictate that "in some circumstances we're not allowed to notice, we're not allowed to eavesdrop, and in others we can."

Weinberger points to walking down the street and encountering people engaged in various sorts of social interaction, each of which "comes with its own set of norms about privacy, which competent, non-crazy citizens understand and obey." If two people are engaged in conversation, he says, "the norms are quite clear about whether you are allowed to listen to them or not." In fact, you *are* allowed to listen (you often can't help it)—"you're just not allowed to *notice* it."

Failure to comply with these norms can be hazardous. For example, on an airplane earlier this year I couldn't help noticing that the man across the aisle from me was having a high-testosterone business conversation on his cell phone (we were still at the gate). The passenger directly behind him bravely, if imprudently, interrupted to ask if maybe

Lew McCreary (lmccreary@harvardbusiness.org) is an HBR senior editor. He was formerly editor in chief of *CSO* magazine, which covers a wide variety of security and privacy issues.

Background: Great and Not-So-Great Landmarks in Privacy History

Privacy Enhancement

- Fences, walls, shades, and blinds.
- Cash, which confers the benefits of anonymity on commercial transactions.
- Sealing wax.
- Steganography—a variety of techniques (invisible ink is one) for hiding unencrypted text.
- The Bill of Rights.
- An 1890 article in the *Harvard Law Review* by Louis D. Brandeis and Samuel D. Warren. The authors argued that individuals have the right to an "inviolate personality" and a broader "right to be let alone." (Jeffrey Rosen discusses the article at length in his book *The Unwanted Gaze*.)
- The 1980 Organisation for Economic Cooperation and Development privacy guidelines: aimed at "harmonizing" the privacy laws of member nations so as not to disrupt the transborder flow of information required for economic development.
- Electronic Communications Privacy Act of 1986: extends protection against warrantless wiretaps to computer communications. (Does not prohibit employers from freely accessing employee communications over corporate computer networks.)
- Employee Polygraph Protection Act of 1988: prohibits employers from subjecting current or prospective employees to lie-detection tests. (Government agencies and contractors and some others are exempt.)
- In March 1999 President Bill Clinton appointed Peter Swire, a professor at Ohio State University's law school, the federal government's first privacy official.
- In 2003 Nuala O'Connor Kelly was named the first chief privacy officer of the Department of Homeland Security. (She stepped down in 2005, winning praise from privacy advocates for having done her best despite obvious institutional constraints.)
- In June 2003 the Federal Communications Commission inaugurated the National Do Not Call Registry. To date, more than 157 million phone numbers have been listed.
- In July 2003 California Senate Bill 1386 mandated that security breaches compromising citizens' personal information be disclosed as soon as they are detected.
- In 2005 IBM announced a policy forswearing the use of employees' genetic information in hiring and benefits decisions. In May 2008 legislation with provisions similar to IBM's was passed by Congress and signed into law by George W. Bush as the Genetic Information Nondiscrimination Act.

Privacy Erosion

- Spyglasses, binoculars, telephoto lenses, spy satellites—technological enablers of surveillance, reconnaissance, and espionage. (Critics today object to the fact that Google Earth and Google Maps now feature "Street View" photos of private homes, sometimes even revealing the occupants within.)
- In 1763 soldiers of King George III confiscated John Wilkes's private diaries from his London home. In *The Unwanted Gaze*, Rosen writes that this and other government invasions of privacy inspired the Bill of Rights' prohibition against unreasonable search and seizure.
- Credit and debit cards, which engender digital records of individual transactions. Researchers are looking for ways to restore anonymity to these transactions, perhaps by using trusted third parties, as in the PayPal model.
- The invention of spam. The earliest known spam e-mail was sent to 393 recipients in 1978 over the internet's forebear, ARPANET. (The sender was publicizing the launch of a new Digital Equipment computer.) By some estimates, spammers now send in excess of 100 billion messages a day, but the once-exponential growth rate of spamming has tapered off in recent years.
- The internet, which was developed within a trusted community of academic researchers and established without privacy standards.
- In 1999 Scott McNealy, a cofounder of Sun Microsystems, was famously quoted in *Wired* as saying, "You have zero privacy anyway. Get over it."
- The USA Patriot Act of 2001: made it easier for intelligence and law-enforcement agencies to monitor communications, conduct surveillance, regulate financial transactions, and tighten standards for admitting foreign nationals into the United States. The legislation, written and quickly passed in the long shadow of the 9/11 attacks, reflected a new emphasis on security as an urgent priority surpassing other social values.
- Any point of failure in a giant database makes it vulnerable to breaches. (After 9/11, Oracle CEO Larry Ellison offered to develop the software for a single identity-card database to help fight terrorism.)
- Retailer loyalty cards—the key to accumulating information on what you buy.
- An increasingly pervasive surveillance culture. London alone has roughly 500,000 CCTV cameras—42 of them reportedly within a block of the flat in which George Orwell wrote *1984*.
- Breaches at TJX and other companies, some of which had grossly inadequate security measures or had retained sensitive information that should have been purged.

the guy could take it down a notch. “Hold on a second,” said Testosterone Man into his phone. “I got some jerk talking to me.” Then he spun around in his seat and instructed his fellow passenger to “sit the hell down and shut the hell up” (or words to that effect).

According to Weinberger, we are now in the midst of a widespread cultural adjustment involving privacy. New technologies upheave old norms, and new norms need to be negotiated—a process that takes time. If the social contract obliges us to ignore some of what we learn in public settings about others’ private lives, new technologies can mightily complicate that obligation.

Who Speaks for Privacy?

When a hiring manager Googles a job candidate (see “We Googled You,” HBR June 2007), Weinberger says, “Google will find every mention of the person, including stuff that if you were walking down the street and stumbled upon you would just ignore. Google does not do the ignoring for you. It’s all presented and has equal weight: the Boy Scout merit award and the arrest for urinating in public. Because that’s how information is—it’s all just bits—and the software can’t make those decisions for us.”

All Google results are juxtaposed: the Boy Scout merit award and the arrest for urinating in public.

Because Weinberger sees privacy through a social lens, his solution to the problem of Google’s indiscriminate presentation of information is that consumers of search results should learn to ignore unwanted or immaterial information: “What I’m hoping is that businesses will develop more of a sense of forgiveness” and put the results in perspective. It’s a learning process, he says, because the juxtapositions—merit badges, public urination—are potentially jarring. “We’re so used to accepting a squeaky-clean, self-constructed résumé as a representation of a person, but that has little resemblance to the flawed, messy selves that we all in fact are. So here we have this disgorging of information that is without regard to seemliness.”

Jeffrey Rosen knows something about what’s seemly and what’s not. Rosen, like Daniel Solove, is a professor at George Washington University Law School. He writes about threats to privacy in his books *The Unwanted Gaze: The Destruction of Privacy in America* and *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*. At the center of the former is his analysis of the Kenneth Starr investigation, which ultimately led to the impeachment, trial, and acquittal of President Bill Clinton. Rosen credits Starr with having focused attention anew on “how little our legal system cares about privacy today and how much more robustly intimate secrets were protected in the not-so-distant past.” Starr, says Rosen, was operating according to relatively new norms suggesting that the private conduct of public figures is fair game for public exposure.

Rosen writes about literal exposure in *The Naked Crowd*, beginning that book with descriptions of two actual prototypes for a passenger screening machine: The “naked machine” sees through clothing to produce an anatomically exact image of the person being screened; the “blob machine” produces an amorphous, desexualized representation of the person. Both versions capably do what they were designed to do: detect concealed weapons and other security threats. Rosen insists not just that it’s preferable to pick solutions that best protect privacy, but that privacy protection should be built into every process and technology. Indeed, the thesis of his book is that most if not all important security objectives can be achieved without unduly compromising privacy.

But someone will always have to speak for privacy, because it doesn’t naturally rise to the top of most consideration sets, whether in government or in the private sector.

There’s a reason for that. The privacy writer and researcher Alan F. Westin famously created a bell curve showing how concern about privacy has changed over time among three groups: fundamentalists (absolutists of the Logan Roots camp), pragmatists (those who worry about threats to privacy but believe that reasonable safeguards are in place or can be created), and the unconcerned (those who give privacy little thought). In Westin’s surveys, fundamentalists made up only 15% to 25% of those polled.

“I guess if I have an evangelizing message for business,” Rosen said in a recent interview, “it’s that companies can’t expect that the public debate will solve all their problems. They’d do better to behave proactively and devise data-sharing and -collection regimes that won’t get them into trouble down the line—both because that’s the responsible thing to do and because they really might be embarrassed if they don't."

Chief *What* Officer?

Some businesses internalized that message a long time ago. Harriet Pearson is IBM's chief privacy officer, a role she assumed in 2000, when Lou Gerstner was CEO. Gerstner was "convinced that as the Web emerged as a business platform, companies—particularly one such as IBM—had to lead on privacy," Pearson says. "We were at an inflection point with respect to the pervasiveness of technology in business processes, and he correctly judged that IBM needed to use its leadership on that issue to support our initiatives on e-commerce."

Pearson spent her early career as an engineer for Shell Oil, went to law school, practiced environmental law for a while after graduating, and joined IBM's government-affairs office in Washington in 1993. With no background in privacy issues, she delved into IBM's internal files on the subject and discovered that the company had hired the young Alan Westin in the 1960s to help it develop global privacy principles to govern human resources practice. As a result, at a relatively early date IBM "majored a lot on workforce privacy," Pearson says. "We were among the first to say that when we're interviewing an employee for a job, we have no reason to ask about their religion, what country club they belong to. Those questions used to be commonplace. And we said no, that's not relevant."

In 2005, under Chairman and CEO Sam Palmisano's leadership, IBM adopted a forward-looking global policy that forswore the use of employees' genetic profiles in making decisions about hiring or access to health insurance and other benefits. Pearson credits IBM's own "DNA" in issues of employee privacy and nondiscrimination for the logic behind its policy on genetic profiling. "There's a direct line that I can draw back to our history in the 1950s and 1960s that is consistent with who we are as a company," she says. (In May 2008 George Bush signed into law the Genetic Information Nondiscrimination Act. IBM's early support facilitated its passage.)

IBM's manifold adventures in new technology—including systems for accelerating genomic research and pharmacological innovation—enable it to foresee developments that have implications for privacy. Pearson says it's part of her job to scan company and industry horizons for potentially gnarly situations: "My business needs make me as likely, in one day, to be looking at genetics and RFID, and what they mean for privacy issues, as at data privacy and security issues associated with global business processes and the emergence of what's being called 'cloud computing.'"

IBM sees revenue potential in RFID but also understands that it's a controversial technology from a privacy standpoint, Pearson says. "So we have worked in a number of places—including technical standards, but also with policy folks here in DC—to create best practices for the implementation of RFID. And we've recommended these to our partners in business. Although we ultimately do not control how these technologies are implemented, we can sure influence our part of the ecosystem. It is in our interest to do this, just as I would argue that it is in the interest of enlightened business leaders to consider where their business models intersect with this human need—human expectation—for privacy, and the legal obligations that they may have, and figure out how to make the connection in a good way." (See the sidebar "Privacy Checklist for Business.")

About seven years ago Pearson found herself at an informal gathering with half a dozen other privacy executives. The positions they occupied were in many cases newly created and not well defined (some had broad responsibilities, whereas others dealt mainly with compliance), and they all found it helpful to compare notes and share ideas. They decided to start an organization—now known as the International Association of Privacy Professionals (privacyassociation.org)—whose membership has since grown to more than 5,000.

That growth rate reflects more than just a greater appreciation of privacy protection as a business responsibility: The stakes of failure have ratcheted up. "Before 2004," Pearson says, "you could collect people's information and do whatever you wanted to with it, within reason. If it fell off the backs of trucks, or if it got lost or penetrated, no harm, no foul. Nobody needed to know." Now almost *everybody* needs to know.

In 2003 California passed legislation mandating breach disclosure for businesses with customers living in the state. Companies were obligated to alert them to a breach at the earliest reasonable moment after it was discovered. Since then, most other states (close to 40 and counting) have adopted similar measures, adding to the corporate compliance burden and moving privacy protection to the foreground. "It has fundamentally shifted the risk equation," Pearson says of this spate of legislation. Apart from the costs of notification, mandatory disclosure exposes businesses to reputational damage that is no less real for being difficult to calculate.

Exhibitionism as Opportunity?

It would be hard to prove that people now assign a lower value to their privacy than they did in the past. But attitudes toward privacy are shifting, abetted by new technologies—some scary and others exhilarating—that generate new threats to privacy and new forms of online self-exposure that appear to disregard them. YouTube and Facebook teem with private lives recast as performance art. Is this a phenomenon that businesses can freely exploit?

If, says Pearson, "your bent is an operational and risk-management one," it becomes a question of "how to minimize your risk and balance that with your need to have this information." In other words, will pursuing a particular opportunity do the business more good than harm, or vice versa?

Jim Buckmaster, the CEO of the successful classifieds website Craigslist, describes erring on the side of almost total nonexploitation. "There's all kinds of things that we don't do," he says, "and the short answer to why we don't do them is that we're as close to 100% user driven as you can get. The reality is that users don't ask us to analyze their behavior patterns."

Buckmaster and Craigslist founder Craig Newmark have raised eyebrows by declaring

In Practice: Privacy Checklist for Business

by Harriet Pearson, IBM's chief privacy officer and a vice president of its Legal and Regulatory Affairs group

- **Align privacy with strategy.**

It is especially important for businesses that have highly valued brands or that compete in information-intensive industries (including health care, finance, and high tech) to take a leadership stance on privacy and data protection.

- **Look beyond rules to values.**

Embedding privacy and security values in your corporate culture will yield a bigger return than the most comprehensive set of rules. When values are developed from the bottom up, they will be lived, not just recited.

- **Anticipate issues.**

It should be someone's job to scan for products or practices in your business or industry that raise legitimate privacy concerns, and to collaborate with stakeholders to develop reasonable solutions. Be prepared to work across the industry as well as internally.

- **Create accountability.**

The role of a privacy or security officer is to unite and coordinate efforts across silos. All those involved in setting and implementing information policies, including the head of HR, the CIO, and the marketing VP, are potential participants—but someone has to be accountable.

- **Don't conflate security and privacy.**

Getting privacy right in a business context means meeting societal or regulatory expectations for what type of information is collected, how much, with whom it's shared, how it's used and protected, and how long it's retained. Resist the temptation to focus solely on data security.

- **Treat privacy as a social responsibility.**

In globally connected, information-rich societies, privacy and data protection belong on the corporate citizenship agenda alongside the environment, diversity, and other important issues.

- **Manage your data supply chain.**

Data-handling obligations flow with data that cross corporate or national boundaries. Business ecosystems that include global sources of talent and services need standards for data management that can rationalize an international patchwork of expectations and regulations.

- **Rely on technology when appropriate.**

It can't substitute for leadership, common sense, and good policies, but simple tools (automated checklists, encryption, audit logs) can do wonders to enable compliance. And emerging capabilities—face masking in digital surveillance systems, privacy-preserving data mining—can help resolve conflicts between information use and privacy.

- **Plan for disaster recovery.**

No information system is fail-safe. In case of a data loss or breach, have a rehearsed response that addresses technical, individual, legal, and other needs.

- **Heed both boomers and millennials.**

The under-25 crowd is not dismissive of privacy, but it does embrace online, collaborative work and play. Your privacy thinking must span a range of generational norms and expectations. One employee may freely post pictures and personal information online but recoil from having an employer or the government collect a biometric for identification, while another does just the opposite.

that their company is uninterested in maximizing revenue. Defaulting to an extremely conservative position on privacy is thus fairly straightforward for them. "Most companies are trying to maximize revenue, and you can make money from people's personal information if you care to," Buckmaster says. "Since we're not trying to maximize revenue, we really have no incentive or interest in doing that. So we don't have the kind of conflict of interest that most companies do have."

The Craigslist perspective is useful mainly as a bracing counterpoint to normal: Few companies can duplicate Buckmaster's nullification of the usual risk-management calculation. Facebook, for example, ran afoul of this calculation late in 2007. Its default position was that the product preferences Facebook users expressed to their friends could be freely shared with advertisers. The company had guessed wrong about whether its users would mind; it had to change the default from yes to no and introduce more-aggressive privacy protection on the site. The lesson? When friends exchange information as a form of social lubricant, they see its appropriation for commercial purposes as an invasion of privacy.

A Generation Gap

What matters in the realm of privacy may be generationally colored, with attitudes shifting over time. I came to consider this possibility after a personal epiphany involving the proliferation of surveillance cameras. Several years ago my mother and I were watching a CNN segment that showed surveillance footage, taken in a Wal-Mart parking lot, of a woman smacking her child around in the backseat of her car. We both found the scene troubling, but for very different reasons. Whereas I was appalled at the woman's behavior, my mother was shocked that the camera was there to witness it. (I can't say I approve of the spread of cameras into public spaces, but I've come to accept them as accessories of modern life.)

My mother, animated by a libertarian streak, worried about cameras invading her privacy. I, like many parents, worry more about the apparent epidemic of self-exposure among younger citizens of the internet as they post their party videos and snapshots, thereby generating potentially troubling future Google search results. Can people invade their own privacy? When, not so many years from now, HR apparatchiks go fishing for the indiscretions of would-be hires, will they have developed the sophisticated forgiveness that David Weinberger proposes?

Harriet Pearson has a Facebook page. So do many of my colleagues. So do I, for that matter. To the dismay of my daughters and stepdaughters and their legions of college-age peers, elders have colonized growing outposts on social networks originally conceived exclusively for the young. The *Lord of the Flies* world of social networking is at last getting an influx of adult supervision. How will that accelerate—or at least affect—the emergence of social norms with respect to privacy?

It may be that Google-search forgiveness will come naturally only to the digital-native generation. The rest of us will have to unlearn older ways. Time will normalize the consequences of this social change as it has of all others. Meanwhile, small chattering tribes of "friends" will happily share the names of their favorite books, movies, bands and songs, brands of beer, lipsticks, condoms—and many other things worth caring about if you're a marketer looking for insights or a "coolhunter" looking for undiscovered trends.

Jim Buckmaster finds the social-networking phenomenon inspiring in its adventurousness. "Kids are having a lot of fun with social networking. For a certain personality type, it may be easier to connect socially with the aid of an internet site than in the real world. In that sense, I think it's probably a great thing."

Nonetheless, Buckmaster likens teenagers' online excesses to the perennial problem of young drivers who flirt with disaster. "People's appreciation for risk doesn't fully develop until they're in their thirties or maybe forties. You see that all over the place. With respect to driving automobiles, there just isn't any way of getting around the fact that 16-, 17-, 18-year-olds are a lot more likely to get into a serious accident than someone who's 30 or 40. And part of that's due to their inability to appreciate risk." As young people age, Buckmaster believes, their attitudes toward risk will change.

"I don't know that one can be judgmental about it," Pearson says. "It's just that it's happening. From a businessperson's perspective, what does it mean? It's huge. If you're building business models to take advantage of online advertising, or trying to get closer to consumers, it's a huge opening." However, she hastens to add, potentially confounding privacy nuances need to be worked out.

Working Out the Nuances

Part of the solution lies in behavior (individual, corporate, social), and part is technical. The technical part, albeit daunting, is sure to be easier than—but not unrelated to—the behavioral part. When it comes to privacy, technology should focus on compensating for human beings' tendency to follow the paths of least resistance. The rap on internet security has always been that ordinary mortals of modest technical ability can't possibly implement it without the help of an IT department. Thus vast swaths of the online user base do without the robust protections—mainly encryption—that would shield their information from identity thieves.

IBM and a consortium of software vendors (working through the nonprofit Eclipse Foundation) are involved in an open-source project known as Higgins. Higgins enables users to have potentially anonymous online presences that mask their personal information while a reliable third party vouches for their legitimacy—think PayPal for identity. It's designed to be flexible—to go with you from site to site and be adjustable so that you can allow some sites to know more about you than others.

Higgins enables users to have potentially anonymous online presences—think PayPal for identity.

Amazon's algorithms have collected plenty of information about my taste in books, music, and DVDs. Can I trust its employees not to misuse what they know about me? I'd like to think I can, but I don't know for sure. Would I henceforth prefer a Higgins-like disguise when I shop there? Maybe so. But that won't expunge my legacy data from the many sites on which I have disclosed personal information—either indirectly or explicitly. That problem is perhaps less amenable to an elegant solution. The natural temptation for a business is to treat customer data as a serendipitous source of opportunity. But retaining customers' or any other sensitive personal information is potentially costly—and, as TJX and other companies have learned, potentially risky. (In December 2006 some 94 million payment card numbers of TJX customers were stolen by a small band of not particularly gifted hackers.)

Apart from the regulatory hammer of breach-disclosure legislation, what data safeguards can businesses expect to see develop? Privacy attitudes and initiatives may well change in the United States when a new administration takes office in January 2009. But no matter which candidate prevails, Pearson anticipates at least a push to make accessing patients' online medical records more difficult. Likewise, she says, the Privacy Act will probably be amended in an effort by government "to restrain itself from having so much free access to information."

The U.S. Federal Trade Commission has proposed voluntary guidelines to help protect consumers against unwanted privacy violations arising from ad targeting based on online-behavior analysis. Among other things, the guidelines propose that websites that collect data for this purpose should make it easy for users to opt out (as Facebook essentially did when it changed its default option); should provide adequate security for all collected data (and put time limits on its retention); and should collect sensitive data—about medical conditions, for example—only after getting consumers' express consent to receive related advertising. Being voluntary, the FTC guidelines are toothless—and they simply distill the commonsense principles adhered to by most responsible websites. Moreover, privacy researchers versed in the technical issues related to cookies note that security software can render the opt-out process unreliable—data may keep being gathered after consumers think they've turned off the faucet.

Privacy law in Europe is likely to be modified to reflect changing models of information collection and sharing. And we can expect privacy to grow in importance in China, India, and the Philippines—which are ever more tightly knit into the global information flow—as those societies come to grips with the demand for greater transparency as a condition of participation in international markets.

Why Privacy Matters

One might conclude that privacy divides the world into optimists and pessimists. Optimists trust that their information will be treated responsibly and with sensitivity; pessimists expect to be attacked by unethical or exploitative sharks. That notion points us back to David Weinberger. Privacy is less a matter of exerting control over our information than of expecting society to continually evolve solutions that allow us to live together in a more or less civilized state.

Privacy matters because the social fabric depends on it to a great extent. A sophisticated understanding of privacy helps to define the shifting boundaries between public and private spaces and purposes. For example, free speech trumps privacy until it strays into slander or libel, at which point a privacy interest arises. When the radio shock jock Don Imus made racial and derogatory remarks about the members of the Rutgers women's basketball team, a social norm quickly asserted itself. Imus was widely condemned, fired from his job, and shamed into issuing an abject, apparently sincere apology to the Rutgers team. No one was sued (though the threat of a lawsuit may have hung over Imus and his employer); the solution arose swiftly—almost organically—and neutralized some of the transgression's toxicity.

Optimists expect reasonable norms to emerge naturally; pessimists may demand legal or regulatory solutions. Whether or not customers clamor for greater privacy, whether or not draconian legislation waits in the wings, whether or not terabytes of customer data are a golden opportunity, businesses should care about privacy because the general trust in commercial interactions depends on it. If businesses are perceived—either individually or monolithically—as disregarding reasonable norms, customers will notice and react.

Over the years, the most curious thing to me about privacy has been that repeated demonstrations of its fragility have so far failed to provoke a larger, louder hue and cry. Despite ever more dramatic and astonishing examples of abuse, Westin's privacy fundamentalists have remained relatively constant at 15% to 25%, with the rest of us either optimistic or unconcerned. The thing about privacy, though, is that it's an abstraction—right up until your identity is stolen or your preferences are exploited. If Facebook's otherwise happily self-disclosing citizens can get riled up over a mercantile invasion of their data, who can't?

Reprint R0810J
To order, see the next page
or call 800-988-0886 or 617-783-7500
or go to www.hbr.org

Further Reading

The *Harvard Business Review* Paperback Series

Here are the landmark ideas—both contemporary and classic—that have established *Harvard Business Review* as required reading for businesspeople around the globe. Each paperback includes eight of the leading articles on a particular business topic. The series includes over thirty titles, including the following best-sellers:

Harvard Business Review on Brand Management
Product no. 1445

Harvard Business Review on Change
Product no. 8842

Harvard Business Review on Leadership
Product no. 8834

Harvard Business Review on Managing People
Product no. 9075

Harvard Business Review on Measuring Corporate Performance
Product no. 8826

For a complete list of the *Harvard Business Review* paperback series, go to www.hbr.org.

Harvard Business Review

To Order

For *Harvard Business Review* reprints and subscriptions, call 800-988-0886 or 617-783-7500. Go to www.hbr.org

For customized and quantity orders of *Harvard Business Review* article reprints, call 617-783-7626, or e-mail customizations@hbsp.harvard.edu