1

The Seven Sins Against Privacy

Privacy is not something that I'm merely entitled to; it's an absolute prerequisite.

Marlon Brando[1]

Privacy is a common word that is, like most overworked terms, somewhat ambiguous. The *Oxford English Dictionary* defines it as "a state in which one is not observed or disturbed by others."[2] The *American Heritage Dictionary* says it's "the quality or condition of being secluded from the presence or view of others."[3] *Merriam-Webster's* alternatively defines it as "freedom from unauthorized intrusion."[4] But in its frequent press mentions these days, it has taken on yet another connotation. There, it has come to mean the loss of control of personal information, generally because of technology.

A lack of consensus on the meaning of privacy creates equal confusion about what constitutes a privacy violation. Generally violations are measured against a legal template—an act breaks a privacy law; therefore it's a violation. This approach doesn't work well against technology-enabled privacy offenses because they're usually too new to have generated restrictive laws.

Privacy invasion means something different to each of us; it's a moving target. When you hear the term you may automatically think of an invasion by a technology like wiretapping, while others may think about having their identity stolen. To some it's an advertising

annoyance, like junk mail, while to others it's the exposure of private information, which can be demeaning and undermine their dignity. The understanding of privacy can also be cultural and generational, aspects that I discuss in Chapter Seven. Privacy means something different in urban and rural settings. Baby boomers feel that it's an entitlement; Gen Xers don't. Everyone seems to agree that privacy is or should be a right, although, as I will show, there is at best a tenuous basis for that belief. One thing is certain: the idea of privacy has changed and evolved throughout history, never more so than in this complex Information Age. Overall, I see three basic meanings for privacy:

- Seclusion—the right to be hidden from the perceptions of others
- Solitude—the right to be left alone
- Self-determination—the right to control information about oneself

Privacy is at the whip end of information technology. Even a small, incremental innovation can have profound effects on privacy. Take the camera phone, for example. The nationwide trend now is to ban all cell phones from gyms because of the phones' new ability to take surreptitious pictures. The enabling nature of technology constantly changes, transforming the context of privacy tangibly, shifting the underlying meaning itself.

To define privacy adequately requires understanding the extent of information technology. One reason the legal system is so poorly equipped to deal with privacy problems is that this scope is constantly expanding. In Chapter Five, I describe the U.S. legal definition. Many lawful activities that pertain to privacy are distasteful or undesirable to most people. Nevertheless, they are likely to remain legal.

Privacy, like pain, is personal and hard to describe even though the perception of its loss is universal. This lack of consensus about a definition makes discussing the topic difficult. Respecting privacy takes more than adherence to laws; it takes thoughtful ethical reasoning and consideration. When we agree about what is wrong, what is right becomes clearer. To that end, I've created a taxonomy of violations. The harms from lost privacy are considerable. Breaking them into categories, some obvious, some perhaps less so, helps us understand the concept of privacy and appreciate the scope of the potential harm as well as the actual harm. In my taxonomy, privacy violations can be viewed as seven sins: intrusion, latency, deception, profiling, identity theft, outing, and loss of dignity. Each sin is described here, and each description is followed by a "commandment," or ethical guiding principle.

Sin of Intrusion

The classical form of privacy abuse, intrusion, is the uninvited encroachment on a person's physical or virtual space. In the nineteenth century, intrusion often took the form of voyeurism or peeping. In the crowded Information Age, it's become a multidimensional offense, involving each of the five senses. Intrusion may mean being forced to sit next to someone on an airplane who's wearing a cloying amount of perfume. It may be simple voyeurism, as when you step out of the shower and see your neighbor staring across the alley at you. It may be auditory, as when you pull up to a stoplight and hear the booming bass of an amplified car stereo.

Technology has added complexity to the mix of potential intrusions. Miniature cameras and picture phones are inexpensive, popular, and powerful. Hidden listening devices can be smaller than a pinhead. Nicole Kidman found concealed cameras and listening devices planted in and around her home in Australia.[5] Fashion model Kate Moss lost lucrative endorsement and modeling contracts

when she was captured snorting cocaine by a camera hidden in someone's clothes.[6]

> Many were surprised when they found out that by attending the 2001 Super Bowl in Tampa, Florida, they were subjected to a biometric technology called facial recognition. All participants were scanned as they entered the stadium, and the images were then compared with a series of digital mug shots in hopes of capturing some known felons.[7]

Our picture is taken dozens of times a day as we pass by banks, convenience stores, or ATMs. It's taken hundreds of times if we live in a big city; for instance, the average person is caught on a surveillance camera three hundred times a day in London.[8]

> Manalapan, Florida, is located near exclusive Palm Beach and is one of the wealthiest towns in the United States. It has decided to blanket the community with cameras and computers to check every vehicle and driver traveling through the area. Software will run the collected tag numbers through law-enforcement databases looking for matches.[9]

Voyeurism technology has gotten more and more sophisticated. web sites sell remote listening devices, digital optics, scanners for picking up cell-phone conversations, and even infrared scanners that spot body movements through the walls of a house or pick out the figure of a human being through clothing. Snooping software used to track online activities can have legitimate uses like monitoring children, but it can also be used by criminals to secretly collect personal information and harvest credit-card numbers.

The Radio Frequency Identification Device (RFID) is a new kind of technology that acts like a wireless bar code. Geographic Positioning System (GPS) receivers are satellite locating devices that are small enough to be put into cars and even cell phones. GPS

trackers and RFID chips are being incorporated into all kinds of devices and services. The President's Commission on the Postal Service is recommending collaboration with the Department of Homeland Security to look into the possibility of developing sender-identification requirements using RFID technology that would use tracking codes to determine who sends and receives mail through the U.S. Postal Service.[10]

The commission cited the system as a way to improve the security of the postal network, but privacy critics warn that taking away the ability to send anonymous mail will infringe on civil and privacy rights. RFID technology is predicted to be one of the most invasive inventions of our time because it can be used on everyday objects: everything from passports and currency to running shoes and printers (see Chapter Nine).

Libraries are already in hot water with privacy advocates because of plans to institute RFID tracking tags for inventory control. San Francisco library officials approved a plan to implement the tags to replace bar codes and magnetic strips. Critics say the technology could be used to track residents and their reading habits via their possessions because RFID tags could be activated and used outside the library. Several large American libraries already use RFIDs for inventory purposes.[11]

GPS is also being used increasingly in consumer products. OnStar, the popular personal security system for General Motors cars, is also a location-tracking device equipped with GPS. Oregon wants to put GPS devices on all automobiles so it can track cars and levy travel taxes proportional to road usage."[12] The Pentagon is developing a system that will catalogue every car and driver in a city by using cameras and computers.[13] The Palm Beach County School District already uses the technology to monitor its bus drivers, including how fast they drive, where they stop, and whether they respect railway crossings.[14] Taxi drivers in Manhattan are fighting for their privacy amidst plans that would equip each car with a tracking system.[15]

Black boxes installed in more than forty million brand-new vehicles provide a feature not listed on the sticker—invisible surveillance. Without owners' permission or even their knowledge, data on seatbelt use, speed, and destinations are collected on American citizens. Only five states have laws requiring car dealerships to inform buyers of the technology.[16]

The Food and Drug Administration has approved the sale of an implantable human identification chip called the Verichip. Applied Digital Solutions of Palm Beach, Florida, is the maker of the RFID tag. The owner of the company argues that it is more secure to have a device planted under the skin than embedded in a bank card or key-chain dangler, which can be easily lost. The Verichip is being marketed as a security measure for providing access to buildings or as identification for financial transactions. The company says it will have a GPS version soon, enabling it to track people implanted with the device to within a few centimeters, no matter where in the world they are. The potential for abuse with this technology is obviously huge, especially because many people may have chips implanted against their will. The first people to be "chipped" will probably be registered sex offenders and paroled prisoners, but the program could be extended to many others, such as nannies, organ donors, or anyone with a security clearance. Without a cultural push-back on chipping human beings, it will almost certainly occur in the future. In May 2006, Wisconsin was the first state to pass a bill prohibiting forced chip implants in humans.[17]

Already in use in Europe and countries such as Malaysia, smart cards containing computer chips will further increase the amount of digitized personal information available on each of us.[18] Electronic health cards are also just around the corner in the United States, with Great Britain, Australia, and Canada leading the way.[19]

China is set to require new electronic identification cards for all its citizens.[20] By the end of 2006, all newly issued American pass-

ports will be equipped with RFID chips.[21] All these smart cards raise privacy concerns because they will store in-depth personal information, giving companies and the government access to an incredible amount of data on all of us.

Intrusion violations are amplified by the double threat of locational technologies such as implanted chips and enhanced sensing. It's no longer possible for you to control your privacy just by being aware of who's around. Not seeing anyone doesn't mean that no one's watching.

Devising an effective measure against intrusion will be difficult. The easy, if impractical, answer would be to bar, or at least license, intrusive technologies. Several states already restrict use of high-end surveillance technologies to accredited law enforcement. It would be difficult to mandate this restriction federally. The best solution would be to toughen the penalties for sinners who get caught and do a better job of writing the laws so as to cover both the newest technologies available today as well as those that will surely soon be commercially available.

Commandment: *Don't spy on me just because you can.*

Sin of Latency

Because most of the damage to privacy comes from stored information, the harm can be minimized if personal information isn't retained. Excessive hoarding of personal information is the sin of latency. It occurs when custodians of personal information keep information beyond an agreed-upon time. This is one of the most common sins; I've yet to find a company that has established and enforced a data-aging policy.

Latency is subtle; it reaches into the future to tweak your privacy, usually long after you've forgotten that you gave out personal information. Typical sinners are companies that you have a relationship with for a temporary period of time, such as utilities, credit-card companies, and Internet service providers (ISPs). Every time

you open accounts with such companies, they create a database file. Throughout the lifetime of the relationship (and sometimes beyond), service companies attempt to fill their files with any information they can get—at a minimum, personal information from forms like names, addresses, and phone numbers. Many require additional data, like birthdays and spouses' names. Some try to get Social Security numbers (SSNs) or at least driver's license numbers, sometimes claiming that they use SSNs as account identification numbers.

The more information that businesses collect, the likelier it is that they'll be able to match those data to other information at some future date. Unique information that describes a single person is an absolute requirement for marketing databases. Without it, ambiguity may result—Which John Smith on First Street? Until the mid-1990s, a phone number was enough to guarantee uniqueness, but no longer. Most of us have more than one telephone number now and change it more frequently than in the past. The easiest information to match is an SSN because it's guaranteed to be unique.

You might assume that a company will delete your information from its records when you close your account, but most companies only mark your file as inactive. Your file won't be deleted now or at any conceivable time in the future (see Chapter Three). Service businesses like telephone, cellular, and credit-card companies have records on far more people than they have active accounts.

So what can a company do with your information after you are no longer a customer? They can sell it. A consumer record with up-to-date information is worth around $200 for cell phone information. Social Security information sells for $60 and a student's university class schedule goes for $80.[22] Ironically, many companies consider themselves freed from any self-imposed or contractual constraints once the relationship is terminated. Contractually, most can do anything they want with the data once you cancel your account.

An attractive part of e-commerce has always been the ability to monitor consumer behavior. Commercial interests, such as DoubleClick, the online marketing technology company, were initially responsible for institutionalizing online data collection. The company uses cookies, small text files containing unique identifiers that are stored on personal computers and used to monitor online activities and track the ads. Cookies help create an audit trail that defeats the expectation of anonymous web browsing. Most Internet users are unaware that they are tracked and monitored to that extent. In June 1999, DoubleClick purchased Abacus, a company that collects and sells data on offline catalogue customers and distributes print catalogues through the mail; it thus has the ability to merge online with real-world information.[23] Even though consumers never visit DoubleClick's web site, they pick up DoubleClick's cookies at participating third-party sites. The linking of invisible cookies to real-world marketing databases means that you can be identified: name, address, even credit rating, whether you buy something on the site or not.

The company eventually agreed to pay $1.8 million to settle lawsuits that claimed it violated privacy laws by gathering and selling consumer information. It also agreed to limit the life span of new cookies by routinely purging the information collected online and not linking online surfing habits with identifying personal information.[24]

The merger of online and real-world data means that whatever you do on the Internet—searching, purchasing, or just browsing—becomes transparent to hidden watchers who know who you are and where you live. Imagine looking up information on bankruptcy on the Internet and then getting a letter in the mail a couple of days later from a law firm stating that it heard you wanted information on Chapter 11.

Because of the lucrative value of consumer information, the highest scrutiny should be on companies that have the potential to

"touch" millions of customers daily, even if they don't appear to be selling any product or service. Search engines such as Google should top the list. As Google has gained in popularity, its scrutiny by privacy advocates has increased. The company offers a suite of products that, by their very nature, collect a lot of personal information about the individuals who use them. In addition to being able to store every search for future analysis, Google has branched out into new areas, such as Google Maps, Google Earth, and even Google Shakespeare. Google Earth offers detailed satellite imagery of much of the world. In many areas the pictures are detailed enough to see the types of cars parked in driveways.

The large amount of personal data collected by Google, the potential for cross-connections, and the perpetual retention of the information make Google a serious future threat to privacy, regardless of its intentions. Web searching and blogging (using personal web logs) are impulsive, and although each instance may not be revealing, collectively searches and blog entries paint a detailed picture of a person's opinions and interests . . . and Google saves all searches forever.

The public teeth gnashing about Google is not based on any actions that the company has or hasn't yet taken; it's based on the potential for problems in the future. Because of Google's central position in the web (52 percent of all external referrals to most web sites come through Google),[25] most people use Google technology, directly or indirectly; this high level of use virtually guarantees that Google has information on almost every person in the Western world.

Because Google saves the results of consumer searches for a long time, perhaps forever, and because it has the search string and Internet address of many searchers, it can do real damage with database matching, which involves taking information from one context, like searching, and equating it to an unrelated venue, like product shopping on an e-commerce site or commenting on a blog. The only requirement is a shared piece of information, a key field that can be

matched between databases. Its gmail product looks at the content of emails so that Google can serve up targeted banner ads. Google Desktop and related products index material stored on home and office computers. If Google were willing to exploit this information, it would become the biggest commercial threat to privacy in existence. The danger exists because of Google's indefinite retention of information coupled with its ability to cross-index many types of stored personal information. If the record of each transaction were purged after a short time, the menace would be greatly diminished.

In 2006, Google was involved in a legal battle with the U.S. government over its search history.[26] The Justice Department had subpoenaed a chunk of Google's log files to make the case that pornography constitutes a substantial part of Internet searching. Google had refused to comply with the order. A judge ruled in Google's favor, requiring it to turn over only a limited set of information with identifying notations stripped off. This case brings home the point that the company is in possession of huge amounts of information that could cause privacy problems if misused by the government, a hacker, or Google itself. Google provides no guarantee, contractual or legal, that such misuse will never occur. In the meantime, it keeps collecting information, apparently deleting none of it.

The more information that a company collects, the likelier it is that some of it can be matched to data saved elsewhere; and the more information that's matched, the deeper the insight gained. The lack of commercial data-retention policies and procedures turns this situation from an annoyance to a danger. Company privacy policies should address this issue, but they never do. Few companies state their long-term data-retention intentions in writing for a very simple reason . . . : they don't have to. This area absolutely requires government intervention: mandatory data-erasure policies enforced by fines for noncompliance. Companies should be legally required to purge consumer information after some minimally necessary time, which could be as little as 180 days from termination of the relationship. Firms that are found to keep data beyond the agreed-upon date could be

sued. In such cases, data, including back-up tapes, network caches, and hard-copy printouts, must be purged completely and throughout the enterprise. Maintaining privacy in the era of digital information requires vigilant data destruction.

Commandment: *Thou shall erase my data.*

Sin of Deception

When too much electronic information is available in databases, the temptation for marketers to use it becomes great. Using personal information in a way that was not authorized by the person involved is the sin of deception.

If a company asks for personal information, it should state how long it's going to keep it, what it's going to do with it, and whom it's going to give those data to. When we give our information to a company, we are entering into a contract with them, just as we do when we lease a car or buy a house. Unfortunately, few companies see it that way. Most retain the right to sell your information or use it for other purposes under certain extremely broad conditions. You lose all control of your personal information if you don't know who has it and what they're going to do with it. The idea that you have the right to control information about yourself is a basic one. People in some cultures, most notably Tibetans, refuse to let anyone take their picture because they believe that the camera steals their souls. I wonder how they'd feel filling out a credit application.

If a phone company asks for your SSN so that it can run a credit check to turn on service, it shouldn't be able to use your SSN later to prequalify you for an unsolicited offer from a third party or to try to sell you another product. The company ought to purge the data after the initial qualification, but it does not. Some credit-card companies give these transaction data to businesses, providing comprehensive snapshots of cardholders and their spending behavior, including where and what they bought, at what time, the amounts of the purchases, the addresses of the stores, and even the demo-

graphic data either given to them by the customer or derived from the purchase history. Without notice and a chance to opt out, individuals have no say over the disposition of their personal information or awareness of how it is being used; they thus have no privacy.

Sometimes the courts can help. Wells Fargo was sued for selling its customer data to third parties, and a California Superior Court approved the settlement.[27] GeoCities, the web-community builder, was also sued for third-party selling of customer information. In this case, the company sold it to direct marketers without permission.[28] Several lawsuits have been filed against data broker ChoicePoint for the selling of personal information to identity thieves. In one case, ChoicePoint neglected to ask 140,000 individuals for permission and directly profited from the sale of SSNs and other private data.[29]

Not just commercial firms are guilty; the government is one of the worst offenders. Tax returns are used to gather information that has nothing to do with paying taxes, such as tracking "deadbeat dads" and student-loan scofflaws. With the No Child Left Behind Act the government also requires schools to hand over students' files to military recruiters upon request and without the permission or even the notification of the students or their parents. The phrase *no child left behind* takes on an ominous meaning when the country is at war and facing a severe shortage of military personnel.

Privacy policies sometimes address the deception issue, although they are so weasel-worded they are not an adequate consumer safeguard. One common statement appears to allow the handoff of your information to the company's "partners." As Roy Rogers would have said, *partner* is a pretty big word.

A related sin is the sharing of your information with a third party without your permission. Privacy policies sometimes address such sharing of data, but even if a company agrees to keep the information within its own organization, it can be a meaningless gesture. When you're dealing with AOL, you're dealing with Time Warner, a huge publishing conglomerate. With big or small companies, privacy policies protect the organization, not the consumer.

In 2001, Macy's announced it would sell the personal information it had collected from 1.5 million of its Internet customers, including their credit-card numbers, birth dates, and email addresses. The department store was asking $90 per thousand names, and, for an additional $15 per name, it included extra data such as household income and the ages of children. The company's position was that it had a right to sell the data unless a costumer opted out.[30]

Some cases involving unapproved third-party data sales have gone to court. But because no blanket federal laws prohibit data sales, these actions are usually successful only when a prohibitive contract between the institution and the consumer is in place. Generally speaking, banks and phone and credit-card companies can sell customer data unless they've limited themselves in their published policies.

U.S. Bank and its holding company, U.S. Bancorp, were sued for selling to a telemarketing company customer data that included credit scores, SSNs, credit-card numbers, and account balances. The price tag was $4 million plus a 22 percent commission on sales. The state of Minnesota claimed in the suit that the company was violating the federal Fair Credit Reporting Act. When the lawsuit was finally settled, the bank refused to acknowledge any wrongdoing but did agree to stop distributing personal information to other companies. It also agreed to give customers a way to opt out of data sharing with the bank's affiliates or partners.[31]

Companies should be forced to detail their information policies, specifying exactly what they will do with customer data, guaranteeing that this information will not be shared with other groups, even in the same organization. Terminology like "to notify our customers of special offers they might be interested in" is no restriction. The same goes for statements like "we will share information

only with our strategic partners." It should be illegal for any organization to hand over information to third parties except for administrative functions like subcontracted data handling. Judging by the trend toward ambiguous and consumer-unfriendly privacy policies, the sin of deception badly needs legal policing to be kept in check.

The discussion of this sin has been focused on the knowing mishandling of data. But a huge problem also exists with inadvertent or sloppy custodianship of consumer information, often by the same companies mentioned in this section. The discussion of the sin of identity theft below provides additional information on this problem; more information on data breaches can be found in Chapters Three, Nine, and Ten.

The lack of laws punishing companies for fumbling our private information, either accidentally or on purpose, is appalling. By imposing escalating fines, legislation could easily force companies that want to be custodians of our personal data to improve their handling of those data.

Commandment: *Keep my information to thyself.*

Sin of Profiling

Not only original information needs to be protected. Data derived from raw information also can be mishandled. Misusing derived information is the sin of profiling.

Profiling is an important technique by which useful analytic information is derived from raw data like grocery-shopping histories; studying such transactions helps explain what customers did, but it does not explain what they will do. That's where profiling comes in. By using heuristics or artificial-intelligence technology, organizations can automatically categorize consumers based on rules created by database analysts, psychologists, or just good guessers. These rules enable companies to attempt to predict consumers' future behavior. Predictive intelligence can come only from profiling. Beginning with database merging and enrichment, profiling is

built on a sophisticated form of information analysis known as data mining, using artificial-intelligence software to find patterns and connections of behavior.

Profiling is based on made-up rules. These can be as simple as "people who live in high-income zip codes are likely to buy a BMW" or as complex as "women who buy Haagen-Dazs ice cream twice in a week may be depressed and are likelier to impulse buy" or as stereotypical as "people who have a Hispanic surname make 20 percent less money than the average person in a given zip code." The harm from these guesses is that they may be wrong and, as a result, you may have a great deal of trouble changing your classification, or, even worse, you may not ever know that you've been labeled. Anyone who's ever been unfairly tagged as a credit risk can relate to this sin.

Often the result of profiling is *customer segmentation*, a marketing term for breaking people into groups (usually by demographics) that indicate their buying behavior. Segmentation is the ultimate goal of marketers because they can identify and catch people who are likely to bite at a given lure. Best Buy, the national electronics retail chain, is redesigning its stores around key market segments. They've named one group Jills—the so-called soccer moms who are the primary shoppers for their families but who are intimidated by electronics stores. The stores have trained special clerks to watch for the Jills, give them tailored assistance, and even escort them to private check-out lines festooned with pink and blue balloons with Jill-friendly music playing in the background.[32]

Profiling is a complicated sin. When it's right and inoffensive, it's helpful to the consumer because the softer side of profiling is personalization. When it's wrong, it can be insulting. When it reveals something that you'd rather keep hidden, it's a violation of privacy. The same technology that helpfully recommends a book that you might like could be making other guesses about you that you don't.

Experian is a provider of aggregated consumer information, much of it collected from the sale of magazines and from catalogue purchases. The company claims to have profiles on 98 percent of Americans. One of the databases they routinely sell contains the reading habits and activities of more than ninety million individuals; it covers 274 publications.[33]

Credit-card companies have used data-profiling technologies for decades. I worked with one card company that said it was able to pinpoint when its customers were having life crises such as mid-life depression by psychographically analyzing their buying patterns. Law enforcement uses similar techniques to predict the behavior of high-profile criminals like serial killers.

No laws protect people from profiling systems. Even though credit reporting is thinly regulated, credit-scoring systems (another word for profiling) are not. The most commonly used system, developed jointly by Equifax and the Fair Isaac Corporation in 1989, FICO is used to rate the risk in extending credit to a consumer.

Because of the credit-scoring company's dominant market position, the score is universally accepted as legitimate and factual. These scores are used by nearly all the large lending institutions to determine ability to pay off debt and as an indicator of creditworthiness. Besides providing financial services to companies in more than sixty countries, Fair Isaac supplies the ten largest banks in the world with credit scoring.[34] Equifax, Experian, and TransUnion—the big three consumer-reporting agencies in the United States and Canada—rely on FICO scores. Every year, billions of credit assessments are based on FICO numbers, including more than 75 percent of mortgage requests.[35] The higher the FICO score, a number between 300 and 850, the better. A lower score can result in higher interest rates for all forms of credit, but can also be used to deny employment or apartment rentals.

A July 2003 Consumer Federation of America survey found that only 2 percent of Americans knew their credit score.[36] In fact, during a conference, a Fair Isaac employee said that consumers derived no benefit from knowing their individual credit scores, that such information would be meaningless and confusing to them. The panelist went on to explain that the company doesn't want people trying to improve their scores because that would result in consumers' acting differently and thus skewing the company's model—a model that uses an unknown and unregulated mathematical formula to calculate the score.[37]

FICO's creditworthiness assessment is subjective. The analysis is based on facts contained in credit reports, but a study released by the U.S. Public Interest Research Group in June 2004 showed that as many as 79 percent of credit reports had errors, with more than 50 percent containing outdated information or data belonging to someone else, as well as 25 percent containing mistakes serious enough that credit could be denied.[38]

Scoring systems are the unseen accusers in the credit world. A bad score is essentially unchallengeable. You have no legal rights to see your score or understand how it was calculated; yet a bad score can hurt you for the rest of your life: it can keep you from buying a house, deny you credit, or even cost you a job. Setting the record straight in the case of an incorrect or unfair profile is like fixing a bad reputation spread by whispers. It's difficult when you can't confront your accuser directly.

The problems with credit-assessment businesses are thus threefold: the FICO scoring system is a mystery and is at best pseudoscientific; many credit reports that these businesses use for input contain substantive errors that affect the scores; and because there's no legal oversight, the scores are sold and shared everywhere without consumers' permission or knowledge.

Increasingly, insurance companies, Telcos, landlords, government agencies, retailers, health care organizations, and a slew of

other organizations are getting access to credit scores and using them for many reasons having nothing to do with credit.

> In September 2004, TXU Energy in Texas started charging clients with lower FICO scores higher rates for natural gas. TXU claims that the Experian data are an accurate predictor of payment performance.[39]

The government, especially the Internal Revenue Service (IRS) and the Department of Homeland Security, also uses profiling extensively. The IRS has a predictive profiling program called the Reveal System that is used to spot possible tax cheats.[40] Homeland Security has been experimenting with several systems designed to spot potential terrorists by categorizing them based on information like the books they buy, whom they talk to, and where they travel.[41] Catching a terrorist after an attack can be accomplished using conventional searching techniques, but identifying the act and the actor prior to commission takes intelligent software that can make educated guesses.

In an effort to fight terrorism, the Pentagon's Terrorist Information Awareness (TIA) program was designed to sift through data held in ultralarge databases looking for connections and relationships among people. Congress suspended funding for the TIA program in 2003, requiring the Defense Department to describe the project's privacy implications in detail. The program would give intelligence agencies access to every private database in the country. Communication, financial, travel, and medical records would be fed into centralized databases to create profiles and analyze patterns.[42] Although TIA is not operational yet, a scaled-down version will soon be running at local airports. Called the Computer Assisted Passenger Pre-screening System, the controversial program will run investigations of prospective passengers while they wait at check-in counters; it will search through a large number of databases to decide each flyer's risk level.[43] ChoicePoint, LexisNexis, and Acxiom are

just a few of the many companies that will supply airports and law-enforcement authorities with personal data for the program. Presumably bad credit information could translate into a flying risk.

Industry and the government have been on parallel profiling tracks until now. However, their data-mining efforts have begun to become intertwined, with the results from one being fed as input into the analysis machinery of the other. Is a terrorist suspect inherently a bad credit risk? Is a credit threat a possible terrorist? The further that the resulting label strays from verifiable facts, the harder it will be for you to challenge the outcome. The problems that clearly innocent people (like Senator Edward Kennedy) have had in getting removed from the Transportation Security Administration's no-fly list illustrate this difficulty. Chapter Eleven discusses these cross-database issues in detail.

Profiling is just guessing. Developers often gussy up their results with jargon to obscure the essentially unverifiable nature of the process. The penalty for bad guessing is severe—the permanent nature of databases virtually guarantees that any labels attached to consumers by a profiling program can stigmatize them for life. Like actuarial tables, profiling is a statistical game, producing reasonable results in the aggregate but breaking down completely when applied to any particular individual. The potential victims of this kind of privacy violation include schoolchildren who are labeled learning disabled, customers termed bad credit risks because of job hopping, or citizens who are restricted from traveling because of a comment they made or a place they visited long ago or just because they happen to have the wrong name.

The basis of free societies is transparency in process. The ability to challenge an accuser is a fundamental principle of democracies. Profiling is insidious because of its stealthy, accusatory nature. Profiling systems are becoming too prevalent and important for us to blindly assume the good judgment of the companies that develop them. Full disclosure of the rules and score derivations is critical to our understanding and ungrudging acceptance of the process.

We should each have the right to see and challenge any entries made in any organizational database, especially those that label us, like credit scores and government threat profiles. Being categorized secretly with no ability to question and correct the label is not only at odds with the principles of a democracy but is the beginning of the slippery slope toward a closed and repressive society. True democracy abhors secrets.

Commandment: *Don't judge me by your data.*

Sin of Identity Theft

The previous sins are committed by institutions against individuals; identity theft is a one-to-one violation. Identity theft is exactly what it sounds like—a thief pretends to be you and steals your money. This is a modern crime, brought about by easily accessible personal information disseminated by computers. Remote-control robbery is one of the fastest growing crimes that the United States and Canada have ever seen, and it was the crime reported most frequently to the Federal Trade Commission (FTC) between 2000 and 2005.[44] In the electronic marketplace, vendors and customers don't meet face-to-face, so businesses identify a buyer by unique alphanumeric sequences—name, email address, and SSN. Sloppy handling of consumer data by both industry and government makes it all too easy for would-be identity snatchers to get the information that they need (see the descriptions of the sins of latency and deception).

> A New York busboy was caught systematically stealing the identities of everyone on the annual Forbes 400 list. He used the Internet to do the research and had already been successful against Steven Spielberg, Oprah Winfrey, and Ted Turner.[45]

An identity-theft case in New York in which three men were caught stealing millions of dollars from thirty thousand people illustrates how easy and lucrative this kind of crime is and why people

are motivated to commit it: one of the perpetrators was a poorly paid clerical worker at a credit-check agency.[46] At $30 per stolen credit file, the temptation for government workers to set up a side business selling databases is also going to be hard to resist. Such is the case of Jeffrey D. Fudge of Lancaster, Texas. A former FBI investigative analyst, he was charged with eight counts of unauthorized access to files on a government computer and with revealing private information to family and friends.[47]

Identity theft is a relatively recent crime. It's possible because of the vast amount of information available on each of us, some of which, like our SSN and mother's maiden name, is often sufficient identification to access our financial accounts. The easiest way to steal an identity is to use an SSN, yet many companies ask, even demand, SSNs for account information but fail to protect them adequately. Half of all universities still use the SSN as the student identification number. A half million identity-theft complaints were filed with the FTC from 2000 to 2005, with 214,000 in 2003—up 33 percent from 2002. Another 301,000 people reported consumer fraud in 2003, half of which was Internet related.[48] Other estimates put the numbers for identity theft much higher, anywhere from 750,000 to 12,000,000 victims each year. Two Gartner Research and Harris Interactive studies from July 2003 found that approximately seven million people had been victims of identity theft in the previous year—more than nineteen thousand per day. This crime increased by 80 percent between 2002 and 2003, with 49 percent of those polled saying they did not know how to protect their identities from theft.[49]

Business Week estimates that online identity-theft losses in the United States are running about $12 billion a year.[50] In 2003, the FTC conducted a telephone survey of 4,057 randomly selected respondents. Almost 5 percent said that they had been the victims of identity theft in the previous two years, and 13 percent claimed their identities had been stolen over the preceding five years. The FTC

estimated that identity theft costs American businesses over $47 billion per year at an average cost of $4,800 per affected individual.[51]

A variety of techniques are used to steal identities. Phishing involves sending out mass emailings with a message purporting to come from a bank or a brokerage; customers are requested to go to a certain web page and validate their account information. The site is bogus, and the newly entered information is used by the crooks to clean out the mark's account. Phishers don't know which addresses are bank customers, but by targeting a huge mailing list, they're statistically bound to hit some. Phishing is a numbers game. If one person in a hundred thousand falls for the hoax, the crooks make a profit. Similar scams used to be run using postal mail, but such attempts had two drawbacks. First was the cost. A mailing to 100,000,000 people would cost at least $7 million for third-class bulk mail and so would hardly be profitable. Second, it is a federal crime to use postal mail to commit fraud. Phishing and spamming are not illegal in themselves. As a practical matter, few phishers are ever caught; many are located outside the United States and are probably not even prosecutable. (For additional information about phishing, see Chapter Six.)

Identity theft can be perpetrated by any strategy that leaves the thief in possession of enough information to empty out one or more of the target's accounts or, in rare cases, with title to a physical possession that can be sold. A couple who left town for an extended vacation had their identity snatched by thieves who wiped out their accounts, sold their possessions, and even disposed of their house. When the unlucky victims returned, they were penniless, carless, furniture-bereft, and staring at a big pit in the ground where their house used to be.[52]

Identity theft can start at a mailbox or a garbage can. Dumpster diving is a common method for getting a victim's financial information; so is prying open mailboxes. Some thieves are even unethical enough to use obituaries. Rondale Vonkeith Montgomery of

Houston fed the names of recently deceased people to his sister, an employee at a collection agency, so she could check credit histories. If a credit rating was good, the pair bought a sport utility vehicle in the dead person's name. In the end, Montgomery was given forty years in jail.[53] While a young woman from a small town in Utah was working as a Mormon missionary in Houston, a church member falsely acquired her personal information and used it to open sixteen credit-card accounts.[54] Olatunji Oluwatosin was arrested in Hollywood for identity theft. Oluwatosin had pretended to be a business and used ChoicePoint to get access to the personal data of more than 145,000 Americans.[55]

Paul Fairchild, a thirty-four-year-old web developer living in Edmond, Oklahoma, went through a crisis when his identity was stolen. After his credit card was turned down while he was renting a tuxedo for his sister's wedding, he learned that an identity thief had used his name and financial information to buy an apartment building in Brooklyn, run an escort service, acquire corporate credit cards for the business, rent cars, and buy luxury items such as furs, jewelry, and expensive shoes. Fairchild was $500,000 in debt before he knew what happened. It took him two years, working full time to clear his name and financial records.[56] Research shows that victims spend an average of six hundred hours recovering their identity after it is stolen.[57]

Identity theft can cost victims more than time. Michael Berry had his identity taken by a convicted killer, who then used it to spend thousands of dollars on credit cards. Michael still carries the letters that law-enforcement officials provided him with stating that he is not the convicted felon.[58] Ain Jones lost her identity to an imposter who stole her money. Warrants for Ms. Jones's arrest were issued, her insurance premiums skyrocketed, and fraud warnings were attached to every digital record connected to her.[59] An identity thief used John Harrison's SSN and good credit rating to go on a spending spree that lasted four months and cost over a quarter of a million dollars. The crook obtained credit cards, a motorcycle, two

other vehicles, clothing, a vacation time-share, and home improvements. The criminal got three years in jail, while the victim still deals with the financial and emotional aftermath, including post-traumatic stress disorder and anxiety attacks.[60]

There are technical ways to snag a little piece of someone's identity without direct contact: cell-phone cloning, for instance. If an identity thief gets close enough to a person using a cell phone, the thief can copy information about the phone and "clone" a new phone that will bill to the target's account. Account information can literally be dragged out of the air now because of the widespread use of wireless technologies like 802.11 and Bluetooth. A technique known as "bluesnarfing" can tap into a person's Bluetooth gadget and access its information, some of which may be account information. This trick was used at the 2004 Oscars by a security company that conducted an experiment to raise privacy awareness. Standing near the red carpet with wireless laptops, the researchers detected over fifty smart phones whose contents were accessible.[61] In the summer of 2004, near Santa Monica, the same group was able to bluesnarf a cell phone from a mile away, accessing and transferring personal data from the target. A week later, they extended the range to 1.08 miles. During that incident they grabbed the address book and sent a message from the phone.[62]

A thief with access to a network can use a "packet-sniffer" and a pattern matcher trained to look for credit-card numbers to gain access to cell phones. If thieves know enough about their marks, they can figure out their passwords and get access to their cell-phone accounts. Contrary to media reports, password guessing, not bluesnarfing, was used to hack Paris Hilton's Sidekick. Her T-Mobile account was infiltrated because the password she used was something any of her fans would know: Tinkerbell, the name of her lap dog. In her case, the perpetrator posted everything on the Internet, including her entire celebrity address book, business memos, and private photos.[63]

Stories like these get a lot of press that publicizes how easy it is to get at data and steal identities. Yet companies continue greedily

asking for more information than they need and store it in security-challenged computer systems. It's not practical to limit the technologies that make identity theft possible. The only real solution is to improve authentication strategies used by financial institutions. Combining techniques like biometrics and password control works well, although nothing will save the identity of someone stupid enough to give information to a complete stranger.

The first line of defense for deterring identity theft is consumer education. The second is instituting financial penalties for mishandling consumer data. As mentioned above, Congress should enact a graduated set of fines for data breaches. The only good way to force companies to beef up their security is to hit them in the bottom line. A simple system of, say, $2 per exposed record would probably be sufficient deterrence. As small as that amount is, several well-publicized cases in the early part of this decade would easily have generated tens of millions of dollars. The money could go into a national fund that could be used to help victims of identity theft. The potentially large cash penalties would hit database-centric companies like Acxiom, ChoicePoint, and Experian the hardest, rightly holding them to a much higher standard than companies in other industries.

Commandment: *Protect my data as if it were thine own.*

Sin of Outing

Identity theft is the consequence of sloppy data handling, which usually occurs because of a mistake at the data center. However, other privacy violations are deliberate, and when they are, they tend to cut to the core of a person's identity by revealing information that a person would rather remain hidden. This is the sin of outing.

This is a new violation, so new that most people haven't considered it yet. It comes from the slang term for the public revelation of a closet homosexual. It's taken on political significance because of the Bush Administration's apparent unveiling of an undercover

CIA agent. Outing is the unwanted connection of an alias to a real identity.

Outing has special significance in the Information Age because of the common use of alternate identities. Many people, especially young adults who grew up using the Internet, have spent considerable time establishing virtual identities for themselves online. Some are simple handles or aliases that provide a shield that allows them to safely express themselves on blogs and message boards. They prefer pseudonyms because false names give them protection against retribution in their "real" life. Privacy is about controlling all personal information, even that pertaining to alternate identities, because in the areas in which they are used and to the participants—they are real.

Most web sites that require identification and don't collect money just need to know the type of person someone is or says he or she is or would like to be. Usually an attribute is enough, like age, gender, sexual orientation, or profession. Providing personal information like name or address is unnecessary and needlessly exposes the customer to identity theft.

People don't want to use their real names for many reasons. Some don't want coworkers and bosses knowing their religious and political beliefs. Others use pseudonyms because real names indicate gender, which can potentially cause harassment in online communities. Sometimes they're professionals—doctors, lawyers, academics, executives, or politicians—who could face real-world retribution for online opinions. Doctors could be sued for malpractice, as could lawyers. Executives could be accused of stock manipulation, and politicians could be challenged for privately expressing opinions that are at odds with public statements. Fundamentally, pseudonyms provide online privacy protection.

Pseudonyms soon take on a life of their own. Unlike anonymity, they are persistent and the wearers of these "nyms" are as protective of them as ham radio operators used to be of their call signs. For many, these names not only provide identity protection but also

are expressions of individuality. Hundreds of thousands of people around the world play online multiplayer games. Using pseudonyms is customary; they not only add to the role-playing atmosphere but protect the player from potential embarrassment in the real world. A corporate lawyer might feel silly if her partners found out that she was a level 10 Elf on weekends.

The Internet is quickly becoming the water cooler of the Western world. It's where people get their news, express their opinions, write and read entertainment reviews, and even research products before they buy them. People seem to talk more freely behind the informality and guise of an alias than they do when they don't have their identities protected. Identity outing can have a chilling effect on the freely flowing speech and casual conversations that are rapidly becoming the hallmark of the Internet.

Society benefits from open conversation. It's good for consumers to talk about their buying experiences; it's enlightening to read blog postings from people who are ideologically and demographically different; it's therapeutic to be able to blow off steam by bitching about politics. Even more important, institutional abuses are often uncovered by whistle-blowers, many of whom use the Internet.

However, some politicians and companies that have been the targets of anonymous Internet messages that they believe damaged their reputations have a different take on the anonymity of the Internet. There has been a flurry of court cases that try to force website managers to reveal the identity of people posting sensitive or purportedly libelous messages.

Les French, a former employee of Itex Corp, used his pseudonym, Whadayaknow, when he made postings that detailed Itex's earnings, which he said were misstated. The company sued him and he countersued. French was later awarded a $40,000 settlement and used it to establish a fund that others could access if sued under similar circumstances.[64]

Congress passed a cyber-stalking prohibition as part of the Violence Against Women and Justice Department Reauthorization Act. It makes posting annoying messages or sending annoying emails anonymously a crime. It's too early to tell whether this law will be used for prosecution by the Justice Department, but if applied to its fullest extent, it could have a disturbing effect on free speech on the Internet. It will almost certainly curtail whistleblowing, making it more difficult than it now is for Americans to find out about institutional abuses and dangerous public-health situations. Speech on the Internet has become a new check on authorities, filling in the gap left by the growingly docile broadcast media.

Many people lose their jobs for discussing their workplace on the Internet. Mark Jen was fired for using his blog to discuss Google, his new employer.[65] Delta Airlines fired one of its flight attendants because she had posted photographs that the airline considered inappropriate on her personal blog.[66]

A growing number of students (in both high school and college and, in the case of Marquette University, dental school) have been punished for comments made on personal blogs. A twenty-two-year-old dental student was suspended because on his blog he bragged about his alcohol consumption, derided the intelligence of some of his fellow students, and called an instructor "a cockmaster of a teacher" (which is presumably bad).[67]

Blogs are gaining in popularity. The Pew Internet & American Life Project says that eight million Americans had blogs at the end of 2004.[68] Other estimates place the number around twelve million. Blogging is engaged in by all age groups but is most prevalent among those under twenty-five.[69]

Many social web sites, such as MySpace and Facebook, encourage the posting of personal information. Several, like myspace.com, are being looked at carefully by law enforcement as potential hunting grounds for would-be child molesters. Here is another excellent reason for not piercing the pseudonymous veil of bloggers—protection against child abuse and stalking. It's much safer for

children to be able to use untraceable pseudonyms. Outing children and exposing them to real-world predators is inexcusable.

Other people have or would like to have alternative lifestyles that are not illegal but may be frowned on by their community or, in the case of the military, may subject the target to disciplinary action.

> Timothy McVeigh, a highly decorated member of the U.S. Navy, was forced to resign from the military after he was outed by AOL. Someone from the Navy read an email from McVeigh, was disturbed by the screen name (handle), and called AOL to find out his identity. The sailor's dual lifestyle was referred to the Navy, who pressed charges against him, requesting his discharge in 1998 under President Bill Clinton's "Don't Ask, Don't Tell, Don't Pursue, Don't Harass" statute, which was enacted in 1993 by Congress to protect all lesbian, gay, bisexual, and transgender service members.[70]
>
> After his discharge, McVeigh filed a lawsuit that requested his reinstatement in the U.S. Navy; he claimed that his discharge violated Homosexual Conduct Policy procedures because the Navy uncovered personal information about him without his consent and without legitimate authorization. A federal judge ruled that the U.S. Navy was barred from discharging McVeigh for allegedly talking about his homosexuality in an AOL chat room.[71] Reinstated, McVeigh faced a hostile work environment and was assigned to menial jobs like supervising trash removal and painting an office; this treatment caused him to retire from the military.

One of the freeing aspects of the Internet is the ability to communicate by presenting yourself as you wish to be perceived. This form of identity experimentation can be harmless, although some might argue that it protects criminals, who want to hide their identity for reasons other than free speech. The anonymous nature of the Internet does, in fact, make it difficult to catch wrongdoers who hide behind pseudonyms when committing crimes online. Many web-site owners' natural ethical inclination against outing their

members serves to protect the felons and has encouraged some groups to take matters into their own hands and come up with creative ways to out online criminals. Volunteer organizations, such as Perverted Justice, scour the Internet, presenting themselves as underage children in order to entrap adults who prey on children into propositioning respondents who they think are kids. In 2003, a prominent New York rabbi was arrested on a number of charges, including attempted endangerment of a child and soliciting a minor on the Internet. Rabbi Israel Kestenbaum thought he was arranging a sexual liaison with a thirteen-year-old girl, but she was actually a he, an undercover police detective.[72]

Sting operations set up by law enforcement have led to similar arrests. In 1999, the founder of IBeam Broadcasting, William Michael Bowles, pleaded guilty to setting up a sexual rendezvous with a young boy who turned out to be a detective from the Sacramento sheriff's office.[73] Infoseek executive Patrick Naughton went across state lines in 2000 to meet a minor for sex. The thirteen-year-old girl was actually an FBI agent.[74] During the spring of 2005, nine sexual predators were picked up in just ten days as part of an online child-sex sting throughout the Washington, D.C., area. Thirteen undercover police officers from the Northern Virginia-D.C. Internet Crimes Against Children Task Force pretended to be children in online chat rooms, where they were quickly propositioned by sexual predators wanting to meet them face-to-face. The nine men arrested included an electrical engineer, a student, an auto painter, a Christian youth minister, and a volunteer firefighter.[75]

Many people use forums as extended support groups, like group therapy sessions. These forums have a common theme, often medical or psychological, and provide a safe venue for discussion of difficult topics by herpes sufferers, terminal cancer patients, abused spouses, and others. The damage that would be done to the participants by being outed is incalculable, ranging from personal embarrassment to professional ruin. It should be their choice to pick the venue and time for their disclosures, if any.

It should be a crime to out an identity, but practically speaking that will never happen. The pressure to protect children and other innocents by piercing the veil of would-be predators is too strong for that level of blanket protection to be legislated for everyone. Law enforcement will insist that they need to be able to uncover online identities to conduct arrests. Intelligence experts will say that terrorism will hide behind anonymity. It would be difficult to craft laws that didn't hamstring the legitimate needs of agents and investigators.

The solution may rest with the technologists, who will need to develop foolproof ways of cloaking an identity. Several open-source groups are developing ways of accomplishing bulletproof anonymity. A large missing piece of the Internet puzzle is a universal alias system that would protect personal information while allowing users to build reputations and transport them across all web sites.

The next several decades should see a furious battle between privacy technologists putting meat on virtual identities and government agencies stripping them back to the bone. Because identity-masking technology doesn't require huge capital investments, the contest is evenly matched; it's anyone's guess as to the outcome.

Commandment: *I am who I say I am.*

Sin of Lost Dignity

Outing is harmful because it affects a core value—someone's identity. A more common privacy harm inflicted by institutions on their constituencies attacks another core value—self-respect. This is the sin of lost dignity.

This last sin is the subtlest and the hardest to qualify; human dignity is the most difficult possession to protect. Comprehensive privacy legislation is impossible, but even if society tries to craft laws that will close the most egregious loopholes, in some areas uncomfortable, yet fully legal, activities could still happen. There will always be places where technology outruns the law, leaving gaps in

its wake. There will also be cases where an offense is not bad enough to be deemed illegal but still humiliates the victim.

We can easily get worked up when falsified information that ruins a person's reputation is bandied about. But what about cases where information is revealed that is true but is personal, private, and nobody's business but the person's own? How would you feel if your medical records were public, with every silly question that you'd ever asked your doctor in plain view? How about a web site featuring your school essays containing opinions that might be better left in a dusty box in the attic? Information technology can easily dig up enough minute but embarrassing information on any of us to leave us exposed as if we were flapping around in a hospital gown.

Causing the loss of dignity has always been a favorite tactic for breaking down a group's spirit. Military boot camp is founded on this principle. From the first second that new recruits step off the bus, basic training is a deliberate attack on dignity, primarily through loss of privacy. The military takes the doors off bathroom stalls, sleeps everyone in open-bay-style rooms, and subjects recruits to constant verbal abuses while pushing them past the point of physical exhaustion.

The poor are historically subject to a similar kind of violation; lack of privacy is a tool of social control as is its resultant humiliation. A welfare recipient tolerating detailed and personal interview questions or a child forced to use a special brightly colored pass to get her subsidized school lunch is the subject of a public shredding of privacy that is often a blow to dignity, imposed almost as a punishment for being needy. The poor have no privacy. In some cases, the courts perpetuate the idea that poor people don't have the same rights as their wealthier neighbors. In the case of *Wyman v. James*, the Supreme Court used fraud prevention as the grounds for permitting welfare investigators to enter a recipient's home without a search warrant.[76]

Technology is also providing new ways for authorities to keep track of the poor and put them under surveillance. The government

already makes use of SSNs to track individuals receiving welfare, and it wants to take the tracking to the next level by issuing benefit cards to track all purchases.[77] Plans are underway to create homeless management information systems, which will continuously track the homeless and keep extensive personal information in databases to be shared regionally.[78] The likely next step will be RFID monitoring of the indigent, like tagging bears or game fish.

Even those who can afford to sue for privacy violations often don't because they choose to avoid embarrassment and ridicule. Undertaking a public legal battle virtually guarantees that the details will be talked up throughout the community.

> The Rhode Island American Civil Liberties Union sued a police officer in 2002 on behalf of a woman who was arrested on suspicion of drunk driving and was then stripped, searched, and left in a camera-monitored jail cell with no clothes for five hours.[79]

Another type of humiliation and invasion of privacy often occurs when employees undergo urine testing for drugs. To prevent tampering with samples, employees are expected to urinate in front of attendants. Workplace monitoring, in general, significantly degrades dignity and compromises the privacy of employees.

Dignity comes from self-control. Those who maintain their dignity are said to hold their heads high and generally have an air of self-assurance about them. It's difficult to be self-assured when you can't govern what other people know about you and what they will do with the information, and today technology makes it all to easy to publish humiliating information, even pictures and video. Privacy and dignity are twinned, the yin and yang of the human spirit. It takes monumental perseverance to maintain dignity when privacy is stripped away.

Charity, government-assistance, and refugee relief workers should always take their clients' dignity into consideration. Television coverage of natural disasters, like Hurricane Katrina, shows the devas-

tation panoramically but lingers on the contorted faces of the victims, stripped of their possessions, shorn of their pride. It was a tragedy when Princess Diana was surrounded by paparazzi as she lay dying on a Paris street. It was humiliating when a dying George Harrison was coerced into signing autographs for his doctor's children. His family sued because they also saw it as an invasion of his privacy and a slam against his dignity.

The best way to handle this sin against privacy is through cultural awareness and reform. Societies need to police themselves by treating egregious violations of the spirit as repugnant, legal or not. Truly democratic societies should zealously defend the right of their citizens, no matter how impoverished or needy, to wrap themselves in their dignity. Such measures will protect each and every citizen's privacy and will lead to the recognition that privacy is as much a human need as it is a community obligation.

Commandment: *Don't humiliate me with my private information*.

The Commandments

Another way to define privacy is by the negative, by what is left when information about us is not abused. When we are not secretly observed. When the information that we give merchants and government agencies is used only for the stated purpose, then erased. When we are the sum of our actions and are not punished before we've had the chance to make our own mistakes. When our intimate data are protected by custodians with as much care and caution as we ourselves would provide. When we are taken at face value and allowed to tell others who and what we are. When we are not embarrassed or humiliated and do not have our self-esteem taken away.

Information technology enables us as individuals and as a society. But to quote a great twentieth-century philosopher, "With great power comes great responsibility."[80] Just because technology allows us to do something doesn't mean that we should. It's too late to roll

back the clock on the innovations that make possible spy cameras, data-mining software, RFID chips, and the complex social structure that is the Internet. Some new laws will have to be passed to protect us against these technological advances, but companies could stave off future privacy regulation by good-faith self-policing efforts. The ultimate answer is a new way of boardroom thinking—ethical reasoning and consideration of the rights of the individual balanced against organizational needs as part of the strategic business-planning process. Sometimes the law is not enough. Some actions that are legal are harmful, hurtful to each of us and, by extension, to society at large. They are sins for the new millennium, crimes so new that they're not even named, let alone outlawed.

Laws are necessary to stop individual cases of abuse. The moral prohibition against stealing is universally held, yet we still need laws and penalties to keep the peace by providing punishment for criminals. Institutional sinning is another story. Corporate abuse is the real danger. A single privacy-unfriendly policy of a large consumer company can violate more people than ten years of identity theft. If decision makers continue to disrespect our privacy, the prospects for us and them are not rosy. We will continue to lose our privacy until we've had enough. The privacy sinners will suffer under an onslaught of overreactive legislation, as angry constituents demand extreme action from their officials. The increasing mention of privacy-violation stories in the media is a good indicator of the growing public concern for privacy.

As a society, we should view willful privacy violators with the repugnance that we would show a serial drunk driver. Our artifice of allowing corporate privacy pillagers to hide behind an institutional shield must end, and the individuals, both managers and directors of companies that violate our privacy, should be exposed. Tolerating corporate or even governmental privacy intrusions is a slippery slope; allowing such abuses reduces our expectations of privacy and softens us up for future intrusions.

The commandments listed in this chapter are good precepts for the foundation of an ethical approach to privacy with far more depth than a sham privacy policy. The only way to adequately protect privacy, short of a tangled web of regulatory legislation, is to substitute a common sense and thoughtful methodology for privacy protection and to fall back on legal permissibility only as a last resort, not as policy. Just because you can do something, doesn't mean that you should.

Privacy violations are more than just a sin against individuals; they can have a pervasive and deleterious affect on society at large as described in the next chapter. A continued pattern of privacy erosion will hurt us as a culture and limit us as a society.