CHAPTER 9

Privacy in the Age of the Internet

Richard O. Mason, Southern Methodist University
Mary J. Culnan, Bentley College
Soon Ang, Nanyang Institute of Technology
Florence Mason, F. Mason and Associates

Provocations:

1. There can be no individual notion of complete privacy. There can only be a tapestry of privacy, one woven with the threads to which people have assented to de facto.
2. A major challenge of the information age is to establish the proper balance between individual privacy and social participation. Honoring the right to privacy requires that an appropriate means be found for enforcing each individual's zone of inaccessibility.
3. The information age is challenging society's ability to respect a person's right to privacy. The use of IT poses a major threat in gaining compliance among third parties (those without a valid need to know personal information) with respect to privacy rights.

TECHNOLOGICAL TRENDS: IS ETHICS THE CABOOSE?

The provocations with which this chapter begins stem from several observations about the Internet's implications for individual privacy:

- By 2010 a highly detailed trail of every person's moves—wherever he or she might go and whatever he or she may do—will be digitally available, much of the data captured as a by-product of the constant use of electronic communications technology. People will attempt to protect their privacy by means of nearly unbreakable encryption technologies, but these attempts will be only moderately successful.

Privacy, an emerging issue in 2000, will continue to be a major political and social issue.

- In an ideal society, the use of technology is aligned and synchronized with the social system. It thereby serves to produce human well-being and promotes the common good. Experience, however, favors an asynchronous principle: The rate of change of technology outpaces the rate of improvement in ethical reflection. Thus, the development of values, strategies, and policies for achieving the common good lag behind technological innovation. As a corollary, the faster the pace of technological development, the greater the gap between the current state of technological use and our conception of the common good. Technology is expanding exponentially now. Kurzweil, for example, forecasts that whereas $1,000 purchases about 1 billion calculations per second in 2000, $1,000 will purchase about a trillion calculations per second in 2010.[1] Internet usage is also growing rapidly. At year-end 1999 there were approximately 110,000,000 users in the United States and 259,000,000 globally. By 2005 Internet usage is forecasted to grow to 206,550,000 in the United States and a jarring 765,000,000 globally. Moreover, usage will continue to grow after then.[2] E-commerce on the Internet is also growing. In 1999 about $14 billion were transacted in business-to-customer commerce. By 2003 this is expected to rise to $380 billion. Business-to-business transactions will be even greater. These technological trends will exacerbate the problem. The asynchronous principle predicts that by 2010, for example, the gap between the technology that is available and in use versus the ethical, legal, and social agreements required to guide its socially acceptable use will widen. It will be even larger than it is in 2000.

- This gap will affect our human rights to autonomy and privacy. New technologies, especially e-commerce applications, will greatly augment individuals' and organizations' ability to collect and use information about people and their behavior. Accordingly, current threats to privacy will be exacerbated, as the following quotations suggest:

  "People can't be trusted with information about each other, they'll do harm with it."[3]

  "The U.S. is schizophrenic about information privacy, wanting it in theory and giving it away in practice."[4]

  "You already have zero privacy—get over it."[5]

- Nevertheless, there is another side to the privacy equation. The philosopher, Etzioni, puts it this way: "It is about our investment in the common good, about our profound sense of social virtue and, most specifically about our concern for public safety and public health. Although we cherish privacy in a free society, we also value other goods. Hence we must address the moral, legal, and social issues that arise when serving the common good entails violating privacy."[6]

These propositions are illuminated in the following contemporary yet prophetic case.

UNREST AT CD UNIVERSE

Have you ever purchased a CD or a book online and paid for it with your credit card? It's a convenient way to buy things and a lot of people are doing it, millions in fact during the 1999 Christmas session. But, what if somehow your credit card and other personal data seeped out of the system and wound up in some unscrupulous person's hands?

This is exactly what happened at CD Universe, an online music store operated by eUniverse.[7] Sometime toward the end of 1999, a "mysterious computer intruder" who called himself Maxim, a self-identified Russian 19-year-old, claimed to have entered the company's database and copied some 300,000 customer credit card files. The exact method Maxim used has not been disclosed, but Brad D. Greenspan, eUniverse's chairman, stated that he "definitely has CD Universe data." Consequently, Maxim now knows a lot about a lot of people.

CD Universe is among those online companies that have a privacy statement, although the link to get to this statement is rather bland, buried as it is in the lower right-hand side of the home page surrounded by several more glitzy advertisements. "CD Universe is committed to protecting your privacy," the statement proclaims. "We do not distribute, sell or rent your name, email address, or personal information to any third party. If we do give information to our marketing partners it is in the form of grouped statistics." Further down in the text the statement continues, "We collect your name, address, and credit card information so we can fill your order. Our secure server encrypts this information so that it cannot be read as it travels over the Internet."[8]

The provisions of this privacy statement are typical, and CD Universe's intent seems ethical enough. Nevertheless, something went awry. The encryption technology may have been working, but despite that, the site's security was lax. Now Maxim not only has a batch of current credit card numbers but also

probably has access to other customer information that CD Universe uses to manage its customer relationships. A leading-edge online company such as CD Universe undoubtedly has constructed (or is in the process of constructing) a rather comprehensive view of each customer to maximize his or her relationship with the company and to encourage up-selling or cross-selling. Also, much of this data is likely used to determine who the most profitable customers are and is organized to better serve their interests, wants, and needs. All of this personal information is enormously valuable to CD Universe and its parent, eUniverse. It is also valuable to Maxim!

J.R.R. Tolkien once wrote, "It does not do you good to leave a dragon out of your calculations, if you live near him."[8a] CD Universe was living closer to the dragon than its executives realized. The company was ill prepared for the likes of Maxim, who apparently found a flaw in Cybercash Inc.'s ICVerify program, the payment-handling software used by CD Universe. This allowed him initially to charge items to other accounts and to move money around. Then he got another and grander idea: He became an e-blackmailer. Emboldened by the protection of being located in a foreign country—one that most likely does not have an extradition treaty with the United States, such as Latvia or Bulgaria if not Russia—Maxim began communicating threatening notes to various parties by means of e-mail and fax. "Pay me $100,000 and I'll fix your bugs and forget about your SHOP FOREVER. . . . or I'll sell your cards and tell about this incident in news," the ransom e-mail threatens.[9] When CD Universe did not capitulate, Maxim published at least 25,000 pilfered credit card numbers on his Web site, Maxus Credit Card Pipeline. At the instant of its posting, this undeniably personal information was made available to millions of users located all over the globe. (The site was closed down by the authorities on January 10, 2000.)

Highlighted here are several key points about the age of e-commerce and de facto surveillance. The world is replete with dragons, people like Maxim who recognize the value of personal information and who are clever, technologically knowledgeable, and unscrupulous enough to seek it and use it for their own, sometimes nefarious, purposes. The fact that this information can be used for extortion stresses the considerable value that people and organizations place on it. Also, some of the advantages and disadvantages of the global, multinational nature of the Web are underscored. All of this experience points to the extreme importance of consumers being able to trust their online business partners. Meanwhile, the Federal Bureau of Investigations (FBI) and a firm called Security-Focus.com are on Maxim's trail. We do not know what methods they are using to find him, but if they entail an appropriate breach of his privacy, electronic or not, society likely will support their actions. Maxim

has forfeited his right to privacy and anonymity by invading others. Privacy is an important but not inalienable human right.

◆ ABOUT ETHICS AND PRIVACY

Ethics is concerned with human well-being. It emerges out of human relationships. Ethical issues arise whenever one member of a society, in the pursuit of his or her goals, impedes or inhibits the ability of another member to achieve his or her goals. The term *privacy,* by one popular description, refers to "the state of being free from intrusion or disturbance in one's private life or affairs."[10] Revealing personal information about someone interferes with their private life, is an invasion of his or her privacy. It thereby creates an ethical issue.

Privacy, in general, may be defined in two senses. It pertains, on one hand, to a member's "negative" right to be "left alone."[11] It also pertains to a member's "positive" right to choose with whom or what he or she will share personal information and who will be allowed to control or interfere in or have influence over his or her life.[12] One's privacy is a function of the social relationships in which he or she participates. Among the crucial roles that people assume in a society that generate personal information and also make them vulnerable to its inappropriate use are customer, worker; global citizen; local community member; and manager of information, such as a chief information officer (CIO).

This chapter focuses primarily on customer-to-seller relationships and only touches briefly on some of the threats to privacy that modern technology poses to people occupying each of the other social roles. In the spirit of Etzioni's "other side of the equation," the chapter also identifies some of the conditions under which one's privacy may be ethically invaded while emphasizing threats that should be thwarted. Etzioni argues that a citizen's privacy may be legitimately breached in situations in which not doing so does great potential harm to the common good.[13] He cites as examples HIV testing of infants, revealing the whereabouts of sex offenders to protect children's safety, deciphering encrypted messages for purposes of national defense and combating terrorism, and the use of certain medical records. Following this line of thinking, a customer's right to privacy may be breached if, for example, it is suspected that he or she has gained access to the system for purposes of hacking or destruction.

The vulnerability of Web sites was vividly dramatized in February 2000. On Monday, February 7, an attack was launched on the popular Yahoo! site by overloading the capacity of the system to respond to visitor requests. The

number of average daily visitors (ADV) to the Yahoo! site is 8.74 million. Using a technique known as distributed denial of service, the attackers used their computer to find other computers on the Internet that were not protected from their incursion. They got access to these unsuspecting computers and made the machines turncoats, instructing them to send large amounts of data simultaneously to the target sites. As a result, Yahoo! was down for 5 hours. Buy.com was struck next (122,000 ADV, down 6 hours). On Tuesday, February 8, Amazon.com (892,000 ADV, down 3.75 hours) was hit, followed by CNN (642,000 ADV, down 3.5 hours) and eBay (1.68 million, down 5 hours). Finally, on Wednesday, February 9, E*Trade (183,000 ADV, down 2.75 hours) and ZDNet (734,000 ADV, down 3.25 hours) were assaulted. The FBI and other security organizations quickly began the process of trying to discover the culprits.[14] Morally, these investigators should be permitted to encroach on the suspects' privacy on the Internet as long as they follow methods of due process, such as gaining a court order when required. But they walk a fine line. The Internet has from its inception been a haven of open and anonymous behavior. Now this very strength has become a weakness. As Etzioni indicates in the previous quote, other goods, such as protection from massive data attacks, can trump a perpetrator's right to privacy. Yet there is a limit. In July 1999 the Clinton administration proposed an extensive plan to install monitoring software on the Internet to protect it from intrusions such as the denial of service attacks. Known as the Federal Intrusion Detection Network, this proposal for preventive action was fought vigorously by civil libertarians who feared that the system would be used to invade corporate and personal privacy. In this age of the Internet, society must continue to balance all of its social values against the important but not inalienable right of personal privacy. This is a global concern as will be discussed in a subsequent section.

◆ PRIVACY IN CUSTOMER-TO-SELLER RELATIONSHIPS

Consider the following vignettes: one a story from an author's past, the second a plausible scenario about a contemporary dot-com company, the third a modern yet credible techno-fictional scenario placed in 2010.

AN EARL YOU COULD TRUST

When I was in high school, my family usually got our groceries from Rapp's Market. This small neighborhood market was located several miles from our house. But my mother frequented the store because Earl Rapp, the owner, was

one of the best butchers in town; he also sought out the freshest produce coming into the Portland docks each day, and he carried a good selection of common groceries. Significantly, and importantly in my mother's eyes, he delivered. Rapp's prices were a little higher than the closer supermarkets' prices were, but for my parents, the quality and service received more than made up for the difference—even in those cost-conscious days when they were bringing up three children with rather ravenous appetites.

Our family developed a fairly remarkable relationship with Mr. Rapp. My mother would phone in an order, usually discussing what she planned to prepare for dinner. The orders were often quite vague:

"Do you have good cuts of round steak?"

"Oh, the tenderloin is better."

"Well, get a few nice cuts for the family. And add some potatoes, some broccoli."

That's when I usually cringed if I was in the room. And so it went. Rapp frequently delivered things that were not explicitly ordered because he thought they would go well with the meal or we might otherwise like them. He was almost always right.

In fact, Earl Rapp knew an enormous amount about our family. He knew when I was playing a football game or performing in a school play. He followed my brother's exploits in baseball and basketball and usually knew what he shot on his last round of golf. He asked about how my sister was progressing in her ice-skating. And he knew where we banked and bought gasoline, who our family doctor was—the doctor's family shopped from him, too—and a lot of other things.

My mother was delighted. Rapp took a big burden off her. My father, who was the agency manager for Prudential Insurance and a staunch advocate of customer service, marveled at the uncanny way Rapp anticipated our needs. He occasionally questioned the price we paid but always ended up more convinced than ever that it was worth it. To each of us, Earl Rapp was a person, a friend, one with whom we were comfortable sharing some of our family's most intimate information.

Why? Over the years I have tried to understand why my parents would make this exception. Although they were outgoing people, my parents clung to their independence and privacy with real tenacity. "It is not anyone else's business." "Don't mention this outside of the house"—an injunction popularized after I ingloriously related some private family matters at my grade school's show-and-tell session. "There are certain things, son, that you just don't tell other people unless you have to." These were house maxims. Somehow, however, Earl Rapp easily and comfortably penetrated the shield.

Contrast this mid-twentieth-century tale with a plausible early-twenty-first century scenario, one not unlike a story about CD Universe as it grows.

IMMEDIATE GRATIFICATION THREATENS TRUST: LUCY STARTS A DOT-COM BUSINESS

Lucy Siegrist and two of her classmates dropped out of the Harvard Business School midway through their first semester to act on an idea they had for an e-commerce company. GetItNow.com, their inspired concoction, is a cyber-store that caters to young, upwardly mobile, two-career families. These people typically are reasonably affluent and have acquired tastes but do not care to devote much time to shopping. When they want something, they want it now. Convenience is paramount. Lucy and her partners have scoured the world to identify and enter into agreements with sources that produce products that meet their intended clientele's purchasing profile. GetItNow.com's prices are set at about 8 to 12 percent below those charged at superstores and, on average, even more below those charged by specialty stores. Due to an agreement with FedEx, DHL, and other carriers, products ordered one day are delivered early the next morning or at a specified time thereafter. A dynamic inventory status system underlies the Web site. Pages are refreshed based on product availability. Hence, every customer is guaranteed delivery of the products he or she orders.

Since the inception of the company, Lucy and her partners have been working 18 to 20 hours a day, seven days a week, frequently sleeping in the back of the dilapidated warehouse they rented to house their servers and communications lines. They eschewed their MBA because they saw a narrow window of opportunity in which they could become wealthy. And they were right! Even though GetItNow.com has never turned a profit—it is awash in publicity, however—the company was recently sold to a large search engine company for $4.5 billion, a price slightly higher than its market capitalization.

GetItNow.com's principle assets are its exceptionally refined customer database, its proprietary software, and its brand name. Using data mining and profiling techniques, GetItNow.com knows what its customers want. Indeed, in a variety of ways it tracks its customers search and inquiry habits—what things they look for and how they navigate through a Web site; their buying preferences by brand, size, and style; and when and in what quantities they are likely to order. This information is used periodically to craft an e-mail message or prompt a phone call to alert customers to a special deal in which they may be interested. Occasionally, unordered goods are shipped to customers with the right of return if they do not want to buy them. GetItNow.com is not very

interested in just processing individual transactions; it is intent on building lifetime relationships. Every effort is made to personalize each customer's experience. Software tools are provided that help each customer self-manage his or her account. On-line seminars, information sources, chat rooms, e-mails, and other forms of interaction are used to build community. The company collaborates with numerous producers of products and related information and is actively engaged in cross-selling. By capturing the time and attention of its customers, it has become a portal-of-preference as well as an information aggregator and a consumer demand fulfiller.

So GetItNow.com satisfies some important and pervasive consumer wants and needs, but at what potential social cost? The company has a far-reaching repository of highly personal information about each of its customers—demographic data, gender, age, wealth, buying preferences, health, habits, friends, and associates—and the list goes on. It captures especially detailed data on each and every move its customers make when they navigate its Web site. Moreover, it is aggressively acquiring more of this type of information. It tries to act like an electronic vacuum, sucking up as much personal information as it can from each transaction and interaction with its customers and site visitors. When it is analyzed, all of this information is potentially quite powerful. Although it can be used to benefit GetItNow.com's customers, it can equally well, under certain circumstances, be used to harm or inconvenience them. Lucy, and now her new partners, possess this power and are able to wield it. Unregulated either by law, social practice, or company policy, the partners can tap into an unsuspecting part of its customers' lives. From a customer's point of view, this open kimono leaves her vulnerable.

Now let's reach out to the year 2010.

A TRUSTWORTHY HOME IN THE FUTURE?

CyberHome.com is an online service that manages your home appliances and other contrivances while you are away or too preoccupied to fiddle with them. Among the things that the site can automatically manage for your home are heating and air-conditioning, security systems, lighting, home entertainment, window shades, and vacuum cleaners—all by means of an Internet connection. Your microwave oven accesses recipes from a database of cooking books and, knowing your preferences and habits, begins to prepare a meal to be ready when you are. Your refrigerator uses bar codes to maintain an up-to-date inventory of the foods it stores, making suggestions about meals, counting calories, and most likely talking to the microwave. In another part of your house,

the e-toilet analyzes the chemistry of its contents, and if certain thresholds are passed, it notifies you and your health provider of the unusual findings. An e-toilet, say, in the case of suspected hypoglycemia, may tell the refrigerator and the microwave to encourage increased consumption. In a serious case, your beeper will tell you to consume some form of glucose now, pointing you to where in the house it is available, including the cookie jar.

Children of all ages who live in a house served by CyberHome.com can play with a large array of smart toys. Each toy has an Internet connection and is modified and reprogrammed continually to meet the children's changing interests, knowledge, and skills. On its network, the company maintains an elaborate psychological and behavioral profile of each child and updates it constantly based on daily activity. This becomes part of the cradle-to-grave record kept on each individual.

This home of the future is possible thanks to a unique service offered by CyberHome.com. By means of numerous communications links (mostly wireless), an extraordinary database of facts and observations on appliances and their use, and programming using advanced artificial intelligence (AI) techniques, CyberHome.com knows a great deal about you and your family and friends. It knows the intimate details of how you and members of your family live your lives, what you do, and when, in every room. Under the control of an honorable and reliable organization, this information can be used to provide numerous, valuable benefits to you and other CyberHome.com subscribers. Personal information about purchasing and financial transactions is threatening enough, but the full array of information that CyberHome.com acquires reaches a deeper level of intimacy. How close are the dragons? Do they lurk in the minds of CyberHome.com's owners and operators? Or are they welling up in the minds of other covetous marketers, eager to buy or otherwise acquire the information—a housebreaker or robber? another Maxim? yours or other governments?

By 2010 all of the privacy dragons will not have been slain. They will most likely have proliferated, given the rich set of technological options at their disposal. As the Internet penetrates more deeply into the fabric of our day-to-day lives, exposure to the dragons will continue to increase. Given the asynchronous principle, the gap is likely to widen. This CyberHome.com scenario—which was inspired by some of the new ideas in home networking presented at the Consumer Electronics Show in Las Vegas during the first week of January 2000—may well become a reality. The gadgets and devices are intriguing, perhaps inviting, but as a society we must pose a profound question: Are we able to shape the context of their use in such a way as to bring

about a good society? If we do not start fashioning the kind of symbiosis we want with technology now, by 2010 or some time not too far distant we will have foregone our opportunity to do so. Such a vision must be grounded on the value of trust.

THE CRUCIAL ROLE OF TRUST

Earl, Lucy, and CyberHome.com possess much the same information about their customers although they acquired it in a different manner. Yet people tend to feel much more uneasy with divulging their personal information (or more likely, having it be acquired by surveillance) to Lucy than to Earl. They may not even have considered at all the consequences of divulging so much information to the likes of CyberHome.com. Insidiously, CyberHome.com's services may be so psychologically rewarding as to result in Huxlian apathy.

What is the difference? Trust. Trust is the key. Both explicitly and implicitly, Earl Rapp was trusted. He treated people as individual human beings and they related to him the same way. Explicitly, his customers knew him to be a man of character, a merchant who wanted to understand them so that he could serve them as well as he knew how and who, like a physician, held information about each business relationship in confidence. Also, families implicitly placed trust in the contained nature of Rapp's small business. It was like a small capsule that let information churn within but didn't let it out. As a decision structure, Rapp's business was comparatively separate, compartmentalized, fragmented, and isolated from the rest of the world. Lucy's, by design, is not. Neither is CyberHome.com's. They are global.

Earl's business existed nearly 50 years ago. Things have changed a lot since then. Very few stores of Rapp's size survive today. Those that have tend to be rather impersonal. Gone, for the most part, are the carbon interlaced 3" × 6" order pads, the barrel-chested National Cash Register at the checkout, the Victor hand-operated ten-key adder, and the manual Royal typewriter in the back room. Gone, too, in large measure, are the in-person touch and friendly way of operating with which Rapp conducted his business. Does Lucy, in her frenetic push to make a dot-com success, place the same personal value on her relationships with her customers and on the details of their lives? For the most part, a digital network complete with scanners, networks, databases, and the World Wide Web has become the modus operandi of grocery store decision structures. Institutionally and technologically, in 2000 we live in a different world than our mid-century predecessors. It is the world of Lucy and

GetItNow.com and soon it will be the world of CyberHome.com. Because we live in this different world, it is all the more necessary that we deal effectively with ongoing human development issues such as maintaining privacy and preserving one's identity.

In this new social context, an individual's lifelong quest for personhood must take a different tack. A person's need for privacy centers not so much on Warren and Brandeis's "right to be left alone"—although this right is, of course, important—as it does on a person's ability to control the direction of his or her life in significant ways—that is, to be her own master, to create and recreate herself as a unique person. Rights, such as our right to privacy, should provide protection for what is necessary to develop and maintain us as individual persons. As stated at the outset, our right to be our own person—our right to freedom and liberty—may take two forms.[15] One is the negative sense that underlay Warren and Brandeis's definition. Our negative right to privacy describes the area in which a person should be left to do or be what he or she is able to do or to be without the interference of others. The second is the positive sense. Our positive right to privacy describes whom or what we allow to be the source of control or interference in our life and whom do we permit to influence what we do. These positive and negative senses of privacy are different from one another, although they may overlap. Yet both are important. Simply put, negative rights describe what information one reveals about one's self, and positive rights stipulate to whom the information will be disclosed. One difference is that the family that Earl served was very much aware of what he knew about them and shared it willingly. It seems unlikely that many of Lucy's customers have entered the same existential bargain. CyberHome.com's customers would be even further away from having arrived at this type of social agreement. A great deal of energy and effort has gone into establishing our negative right to privacy. Many people are aware of and concerned about what information about themselves they disclose and under what conditions. There is still more work to be done both at the policy level and in raising public awareness to protect privacy in the negative sense. Nevertheless, the groundwork is under way.

Privacy in the second sense, in our opinion, has not received quite the same level of consideration. The family was not so much concerned with *what* Earl Rapp discovered about them as, rather, *who* he was and how he ran his business. GetItNow.com, on the other hand, has no such history, no identifiable persona, no clear identity, and no tradition of virtue or character. We know little if anything about its owner's motives and how they are shaped or reflected in the company's actions.

ON DECISION STRUCTURES

We can think of Rapp and his small business as a *decision structure,* a cluster of people supported by technology that carries out the functions of collecting, processing, storing, disseminating, and ultimately using information. Decision structures generate alternative courses of action and choose from among the alternatives developed. That is, they make decisions and take actions, such as delivering groceries or health care or banking services or employment. Decision structures are bound together by values, beliefs, and commitments, all of which work together to form a context in which the information and alternative courses of action are handled and evaluated to arrive at decisions. Almost everything of importance that happens in our lives—birth, schooling, marriage, working, leisure, death, and, yes, day-to-day commerce such as buying groceries or doing the banking—is mediated through one or more of society's myriad decision structures. Life cannot go on, we cannot achieve a full personhood, unless we transact with decision structures. In fact, a rich, Maslovian, self-actualized life can likely only be achieved by interacting with many different types of decision structures. Ours is not a Robinson Crusoe world. Rather, it is replete with a wide variety of decision structures with which we engage frequently. Importantly, we place our trust in decision structures. When we consider our rights to privacy and liberty in the positive sense, our life choices boil down to choosing which decision structures we are going to entrust with our personal information and what information we are going to disclose to them. In effect, we enter into a bargain—a fiduciary agreement—with each decision structure with which we interact. We give them personal information; they hold it in trust and use it, as needed, to provide the product or service they have agreed to deliver.

In general, there are two types of decision structures in our society: helping and controlling. We give our personal information to helping structures such as our doctor, banker, grocer, or electronic home management outsourcer because we want to. We give our personal information to legitimate controlling structures because we have to, because it is required by the regulatory requirements of membership and citizenship in society. In either case, we must trust that these decision structures will use the information to promote, or at least not to harm, our well-being.

Some of our society's decision structures use surreptitious methods to collect information about people, to wit, videocameras on the walls or behind mirrors, miniature cameras installed in ballpoint or fountain pens, satellite or aerial cameras above, hidden microphones, invisible wire-tapping devices, tel-

ephone-bugging devices, electronic dishes that can overhear conversations at a great distance, truth serums, polygraphs, breath analyzers, electronic anklets, voice-stress analyzers, or brain wave analyzers. Many entities also employ the more traditional and open data collection technologies such as scanners, card readers, cash registers, teller's machines, various kinds of sensors, and increasingly, a user's activities on the Internet. All of this data can be digitized and made available electronically.

Many of the decision structures with which we interact today are large and impersonal. Examples include Citicorp, Amazon.com, and Free-PC.com. Free-PC.com gave away thousands of Compaq personal computers in return for the recipients' agreement to disclose considerable personal information about themselves, to receive ads on the Internet, and to have their Web sessions tracked. (As of this writing, however, it appears that the company may be on the verge of bankruptcy.) Seldom in interacting with these organizations do we have a name or a face, certainly not a human handshake, in which to ground our experience. Yet in this electronic age, people somewhat knowingly provide enormous amounts of valuable personal information to these entities. For example, as of the year 2000 over a billion items of bar-coded products are scanned electronically every day, billions of dollars are dispensed by Automated Tellers Machines, and about a trillion dollars careen across the electronic foreign-exchange system every night. Large amounts of personal information move with these transactions everyday. And this personal information comes to rest in the databases of many decision structures. In the mid-1990s Kenneth Laudon observed that "the 400 million credit records maintained by the three largest credit agencies, the 700 million annual prescription records, the 100 million computerized medical records . . . and the 5 billion records maintained and often sold by the Federal government . . . all have real market value that is demonstrated everyday in the marketplace."[16]

◆ DECISION STRUCTURES ARE SUSCEPTIBLE TO INFORMATION TEMPTATIONS

What motivates the members of a decision structure to use personal information? Two books—James R. Beniger's *The Control Revolution: Technological and Economic Origins of the Information Society*[17] and James C. Scott's *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*[18]—discuss in depth how large modern-day decision structures pursue information of all sorts, especially personal information, in

their quest for one central thing: control. Control is the motivation for this type of dragon. It is a manifestation of Nietzsche's will for power. Beniger explains in detail how and why private enterprises collect and process information in the pursuit of profits and economic survival. Information puts businesses in control. It gives them power. He sees economic progress—the prevention of chaos—as the beneficial outcome of this control.

Scott describes how and why governments develop and use information, especially personal information, to execute their functions better. It gives them power, too. Scott, however, is less optimistic than Beniger. He tells a cautionary tale about the dangers of overreliance on the major intellectual and technological innovations of the information age. When he shows how the tools of information control may also be used as tools of violence and imperialism, he tells a morality tale as well. A loss of its subjects' privacy is only one of the questionable outcomes of information-based government actions. Significantly, both authors see these innovations in information and their use as inevitable. The social technological imperative continues: If it is available, it will be used.

So a large number of different decision structures collect and store an enormous amount of personal information that is highly valuable to them and to others in the marketplace. However this gives birth to a potential problem. Possession of personal information creates an enormous temptation to use it, either purposefully or inadvertently. As Jeffery Rothfeder, a former editor for *Business Week,* warned, "People can't be trusted with information about each other, they'll do harm with it."[19] We must consider what any of the many and various decision structures that have information about us can do with it. Rapp had minimal capability to process and analyze the information he had about the families he served. He was involved in a kind of reciprocal bond with his customers and was unlikely to be tempted to reveal the intimate knowledge he held. Lucy, however, may well be more likely to succumb to the temptation. She is part of a revolution in marketing that profiles and targets individual customers in which those who succeed can reap enormous financial gains. If Moore's law[19a] continues as expected, by 2010 CyberHome.com will have access to about 120 times the computing power that was available in 2000. With all of this power at its disposal, it will face a great temptation to use it and apply it to the masses of deeply personal information it collects. Furthermore, the dragons still lurk. Lucy and CyberHome.com are vulnerable to electronic insurgency and to electronic shakedown artists like Maxim. Tragically, they may underestimate the sting of these dragons and what it takes to keep them at bay.

DATA ABOUT EMPLOYEES IS ALSO A TEMPTATION

A temptation to use internal data about employees makes them vulnerable to privacy violations. From the time they fill out their first application form for their employers until the time they leave an organization, employees of all stripes entrust their employers with considerable amounts of information about themselves. Numerous types of automated surveillance, from cameras to recording voice transactions to monitoring e-mail, are being employed. The fundamental issues involving employee privacy are (1) what personal information about an employee is an employer entitled to collect? (2) how may it be collected? (3) how may it be used? (4) with whom within the firm may it be shared? (5) with whom outside of the firm may it be disclosed? and (6) what are the employer's duties for ensuring that the personal information is accurate, complete, secure, and confidential? Related to all of these questions is a concern for how well informed employees are about what information is being collected about them (notice), whether they can limit the information collected (opt-out), whether they can review it (access), and whether they are allowed to change or annotate it.

The technologies that can be used to breach a customer's right to privacy can also be used to violate a worker's right to privacy, including concealed surveillance equipment. In fact, some argue that because organizations have more power over their workers than over their customers—that is, customers are free to leave and do business with other organizations in the marketplace—employee privacy is a more significant ethical issue. The use of computers with Internet connections increases an employee's vulnerability to a breach of privacy. Ford Motor Company, for example, recently announced that the company will provide all 350,000 of its employees with computers to be used in their homes. This will improve computer literacy, but it will also put a lot of personal information in Ford's network that is subject to surveillance. A recent survey summarized the variety of ways that U.S. workers who have access to computers say that they use them either at home or at work or both places: job-related uses (87 percent), e-mail (79 percent), word processing (79 percent), Internet browsing (75 percent), getting news or information (73 percent), games (56 percent, about 15 percent including playing games while at work), shopping (36 percent, about 14 percent including shopping while at work), and paying bills or managing money (36 percent).[20] Questions about viewing pornography, considered by some the largest single use of the Internet, were not included on the survey instrument. Neither was online day-trading, unless some respondents included it under "managing money." Many

organizations consider pornography and online security trading to be unauthorized uses of their computer and network resources. They either monitor for their use—a potential invasion of privacy—or they block access to offending sites by technological means—perhaps a violation of autonomy or First Amendment rights. In the Internet-driven digital economy, information about employees as well as consumers is readily available. Moreover, many new and potent analytical tools are available to be applied to this data to uncover even more about the people involved.

AUGMENTING THE POWER OF INFORMATION

Importantly, Lucy and her ilk have a virtual arsenal of new data analysis tools at their disposal. Today's decision structures have many powerful technologies available to them for handling and drawing inferences from the masses of personal and related information that flows through their organizations. Consider, for example, a set of tools relating to data-warehousing techniques such as relational databases, information centers, decision-support systems, and executive information systems. These tools are being used to develop customer profiles, to infer causes of customer behavior, to depict patterns of customer or vendor activity, and, in fact, to relate personal information to all other kinds of information. Current data warehouse technology performs these analyses more quickly and efficiently than previous methods. Some of these data warehouses are being linked to the Internet or corporate Intranets to facilitate broad and rapid dissemination of the analytical results.

Augmenting the value of data warehouses is the rapidly developing technique of data mining. New correlations, patterns, profiles, and trends can be uncovered by techniques based on applying research in AI, statistics, mathematics, and modeling to large stores of data. Cluster analysis, association rules analysis, neural networks, and decision-tree analyses are among the most frequent algorithms used. These tools are used to relate personal identifying information (such as name, e-mail address, postal address, phone number, fax number, credit card number, Social Security number, driver's license number) with demographic information (such as age or date of birth, family relationships, gender, education, zip code, location, income, preferences, occupation, etc.) and also with transactional and other sources of information revealing habits, purchases, and preferences.

To get the results of these analyses more quickly to a decision maker who can act on them, organizations are increasingly adopting an approach called online analytical processing (OLAP), which is being used to supplement

online transactional processing (OLTP). OLTP supports day-to-day operations by capturing data about people, business processes, and events and storing it in the data warehouses. OLAP is, in effect, a decision-support overlay to OLTP. It facilitates ad hoc queries and just-in-time analyses. In general, OLAP can be used to answer *more* precise questions about *more* people and to get the answers to those who will act on them *more* quickly than OLTP and other methods.

Used individually or in consort, these tools are powerful. But many people do not appreciate the full extent of their power. Consequently, it is highly unlikely that many consumers fully realize what they have actually given up by revealing information to sites such as GetItNow.com or Free-PC.com, even if they did it voluntarily. Their consent may not be fully *informed.* They may be effectively deluded. This is because many of us do not fully appreciate a threat to exposure called *minute description.* Whenever a collection of attributes about a person—A, B, C, and so on—are brought together and connected by the logical connector AND, surprising patterns can be uncovered. A person, for example, may independently authorize a site to collect personal data item A about them innocently enough. The person may then authorize the collection of B with the same indifference. This same person, however, may feel quite uncomfortable about the conjoint data item A and B being revealed about them. Add C and then D and so forth, and the kimono may be flung far more open then they intended or even imagined. The weaving together of each additional attribute reveals more and more about a person until a rather complete and unique description is obtained. The resulting fabric can pose a real threat to one's privacy. As members of intelligence agencies know well, the concatenation of many individually benign attributes can yield remarkable revealing pictures of their subjects. Lucy is poised to do this in ways Earl could never have dreamed of. Technologically speaking, CyberHome.com will be well beyond Lucy's capacity by 2010.

◆ ILLEGITIMATE TRANSFERS OF INFORMATION: A THREAT

The Internet—conceived as an outreach tool—makes techniques such as data mining more broadly useful. This is a double-edged sword: It also exposes users to the Maxims of the world. The Internet has become the lifeline of many businesses, especially through the medium of e-commerce. Today, a large number of Web sites such as CD Universe collect and handle substantial amounts of personal information. But much more than records of purchases of books and music by credit cards is at stake.

The financial services industry presents a foreboding example. In October 1998 at a business leaders spotlight session at Southern Methodist University, J. Gary Burkhead, vice chairman of FMR Corporation and president of Fidelity Personal Investments and Brokerage Group, stated that now that the revolution in consumer-based financial instruments is slowing down, the financial industry is turning to the electronic revolution. Fidelity plans to spend at least a billion dollars a year for at least the next five years on systems and technologies, mostly directed toward the World Wide Web. Burkhead believes that any major financial institution that is not prepared to invest at that level will not be able to compete. Two elements of Fidelity's strategy stand out. Based on information gleaned from customer surveys, interviews, and focus groups, the company plans to develop and offer a variety of self-help financial analysis tools at its Web site. Second, to assist a customer's personal financial management, Fidelity plans to provide automated links from its Web site to a wide variety of other financial institutions. The links will have the capacity to enter the other institutions' databases and extract information such as customer account balances and return it to the Fidelity site. When the full system is implemented, Fidelity customers will be able to log on to their Fidelity Web pages and, using the Fidelity site as a portal, call for their banking and investment information from, say, Merrill Lynch, Bank of America, Prudential Insurance, Metropolitan Life, Allstate, Visa, Glendale Federal Savings and Loan, CitiCorp, and a host of other financial institutions. According to Fidelity's plan, the system will seamlessly collect all of this information and display it for the customer. At this point each customer will be able to initiate transactions and manage his or her overall financial position from a single source, one supported with analytical tools.

This service sounds great! Fidelity has evidence that customers want it. Many other financial institutions are crafting similar plans. But these systems are fraught with privacy pitfalls. For the service to be delivered, a wide range of personal and potentially sensitive information must come together at one time on Fidelity's computers. At that point and subsequently, Fidelity will know a great deal about each of the customers who use this service, including their overall financial status. This creates personal benefit versus personal cost tension in which a customer's privacy is placed at risk. Each customer must make this information available to receive the full benefits of the service. So the key question comes down to, can you trust Fidelity with this information? Will Fidelity treat the information with the same sensitive care that Earl Rapp did? What privacy safeguards are in place? How secure is the system from the dragons? Is the site hackable? Can it fend off a Maxim-type attack? A

denial-of-service assault? Some recent surveys indicate that some progress in being made in establishing privacy warnings on the Web, but the results also reveal that the underlying risk is still widespread.

RECENT EXPERIENCE

Mary Culnan and her associates in the Georgetown Internet Privacy Policy Survey project examined 361 sites drawn from a random sample of dot-com Web sites.[21] The sample was selected during the month of January 1999 from Media Metrix's top 7,500 URLs, which account for about 98.8 percent of the Web's overall traffic. The researchers adjusted the transaction data so that it reflects only unduplicated traffic. Culnan's survey found that 92.8 percent of the sites sampled collect some personal identifying information and that 56.8 percent collect demographic information. Over half (56.2 percent) collect both types of personal information. Only 6.6 percent of the sites collected no personal information.

The Georgetown study also sought information about privacy disclosures. They found that 34 percent of the sample did *not* post any type of privacy disclosure. On the other hand, 236 Web sites (about two-thirds) collected personal information and posted some kind of privacy disclosure, such as the CD Universe statement. Almost 90 percent of these sites provided some type of notice (such as what information is collected, how it is collected and used, whether the site reused or disclosed information to third parties, or whether the site used cookies). About 62 percent of these sites gave the user some choice of being contacted again or having information forwarded to third parties. Less than half (45.8 percent) provided any information about the security of the transactions, whether data was protected during transmission or during subsequent processing and storage.

Cookies, small symbol strings that communicate between a Web browser and a connected server, may be a privacy time bomb. Cookies are resident on the user's hard drive, yet they remain invisible to the user. Upon request by connected servers, cookies collect information that is stored or retrieved by the users' browsers. Obviously, considerable intimate information can be collected about a user by means of these invisible and sometimes insidious cookies. At this time we know very little about how widespread the practice of implanting cookies is or about the many ways in which they might be used to invade our privacy. Some sites using cookies claim that the information will not be used for that purpose. Amazon.com's privacy policy statement, for example, says this: "Our cookies do not contain any personally identifying information, but they

do enable us to provide features such as 1-Click™ shopping and to store items in your shopping cart between visits. Most Web browsers automatically accept cookies, but you can usually change your browser to prevent that. Even without a cookie you can still use most of the features in our store, including placing items in your cart and purchasing them."[22]

A user's service is degraded, however, on many sites when he or she disables cookies. The Georgetown study, like an earlier FTC study, did not collect data about whether or not a Web site actually placed a cookie on the user's browser, although disclosures made about cookies were counted.

A 1999 study of the top 100 sites (all of which had at least 750,000 unique visitors per month) funded by the Online Privacy Alliance had similar findings. Ninety-eight sites collected personal information, 1 collected just demographic information, and only 1 site in the top 100 did not collect any personal information. Seven sites had no privacy disclosures of any type on their site, whereas 59 had both a statement of privacy policy and a statement of the site's information practices. As with the Georgetown study, most of the top 100 sites gave notice and choice in their disclosures, but only about half provide information about security. Lucy has a lot of company, and some of them are not telling their site visitors and customers what they are doing.

Several news items reported in early 2000 show cause for alarm. On January 25, 2000, the New York State attorney general announced that the Chase Manhattan Bank and InfoBeat, a Denver-based Internet company, had been asked to cease routinely sharing personal and financial information about their customers with telemarketing companies and advertisers. In following the practice, Chase violated its own privacy policy and allegedly transferred about 20 items of personal information about as many as 18 million credit card and mortgage holders. Included was information such as customers' home addresses, credit card purchases, finance charges, and available credit.[23] Early in February of the same year, a survey of health care organizations by the California HealthCare Foundation found that confidential information was being disseminated through banner ads and third-party service providers. Numerous potential violations were reported, including breaches by seven members of TRUSTe, the first and largest privacy certification program.[24] Amazon.com announced that it was under investigation by the Federal Trade Commission (FTC) for using software produced by Alexa Internet (one of its subsidiaries), which secretly intercepts personal data and sends it to third parties, including Amazon.com. This information includes entire addresses of each Web site visited and may reveal personal information such as mailing addresses or customer account numbers. Taken together, this

information is used for customer profiling and determining Web-surfing patterns.[25] If these allegations are true, this practice also violates Amazon.com's stated privacy policy.

On February 16, 2000, DoubleClick's stock fell $4.93 ¾ to $106.50 and dropped another 15 percent on February 17 on reports that the FTC was investigating its data collection practices. DoubleClick owns a direct marketing company, Abacus Direct, that keeps a large database on consumer purchases and transactions, focusing on purchases made through catalog houses. Abacus uses software that brings together in one place for analysis data on planning, execution, control, tracking, and reporting activities for use in developing online media campaigns. It was alleged that DoubleClick was unlawfully tracking the online activities of its users and combining customer surfing patterns with detailed personal profiles maintained in the national marketing database at Abacus Direct. *The Washington Post* reported that "Michigan's attorney general said she will file suit against DoubleClick under that state's consumer laws. DoubleClick's consumer monitoring 'is a secret cyber-wiretap,' said Attorney General Jennifer M. Granholm. 'The average consumer has no idea that they are being spied upon,' she said, and that lack of warning constitutes 'a deceitful practice under our consumer-protection act.'" [26] Kevin Ryan, DoubleClick's president, indicated that he was "confident that our [the company's] business policies are consistent with our privacy statement and beneficial to consumers and advertisers." He went on to claim that "DoubleClick has never and will never use sensitive online data in our profiles, and it is DoubleClick's policy to only merge personally identifiable information with non-personally identifiable information for profiling, after providing clear notice and choice."[27] These examples help make another point: Ethical practices with respect to issues such as privacy can be good for business, and poor privacy practices can have a negative impact on a firm's stock prices and bottom line.

The Internet and the Web have become the explosive new sources by which decision structures of all types can acquire personal information and, as the previous reports reveal, they collect large amounts of it. Most sites, like Amazon.com, DoubleClick.com, and CD Universe, provide notice about what information they collect and how they intend to use it. But this is only part of the story. Only about half tell the user how *secure* that information will be. Consequently, security may well be the overriding issue. People want protection from harms resulting from the misuse of their personal information. When this information is widely available, a person is vulnerable to identity theft; credit card thievery; or other physical, financial, or psychological harm. Moreover, as several of the previously cited cases show, some companies, such

as Chase, Amazon.com, and DoubleClick, may be violating their own stated privacy policies. So what is the Internet user to believe?

PRIVACY APATHY

Disclosure, notice, and choice, however, are not enough to protect one's privacy, either in the sense of fending off interference or of choosing one's sources of control, for another psychological reason. As mentioned earlier, few people fully understand the power of such tools as data warehousing, data mining, online analytical processing, and the like that decision structures are using to uncover information about them. Consequently, these people may well give consent without fully realizing the extent of what they are agreeing to. Their consent is either (1) not informed in the sense of informed consent or fair information practices or (2) superficial because they haven't taken the steps to fully inform themselves about the possible consequences. *New York Times* columnist Peter Lewis captures the nature of this unattended apathy:

> Everyday we make bargains of convenience, trading little bits of our privacy for a reduction of hassles. Should we care? Many people seem to think not. And yet, do we behave differently from how we might otherwise, knowing that we are under almost continuous surveillance of one sort or another?
>
> For most people, maybe this is the real issue about privacy in the information age. Perhaps we were so intent on avoiding Orwell's totalitarian Big Brother that we did not notice the arrival of millions of tattletale busybodies.[28]

THE LONG-TERM GLOBAL SOCIAL CONSEQUENCES

All of this presages a major social dilemma. The perceived need for personal information by decision structures to carry out their tasks and to establish control is getting stronger and stronger. An enormous demand for personal information is being generated. At the same time, the acquisition of digital data about people and their transactions is widespread, and the technological means for collecting, processing, analyzing, and disseminating the personal information is becoming more powerful and pervasive. Consequently, the motive, means, and opportunity to violate a person's right to privacy are present. Our privacy can be lost in the negative sense that our lives can be interfered with or without our consent and in the positive sense that we can

unwillingly give up some of the control over our lives to decision structures that are not of our choosing. Etzioni is correct to point out that a right to privacy is not inviolable. It has limits and in special cases can be overridden by other, more socially compelling rights.

One case in point is the approach Maxim likely used: hacking—illegally gaining access to or entering another's electronic system to obtain secret information or steal money. In most parts of the world, it is regarded as unethical. In Singapore it is treated as a serious crime because an offender's hacking tends to undermine the nation's efforts to become a global e-commerce hub. Those caught are accused of "cyber-crime" and usually put in jail. For example, in October 1999 a 17-year-old high school student was incarcerated for four months for hacking into the servers of Swiftech Automation and Singapore Cable Vision. In November 1999 two other youths, ages 19 and 22, were jailed for hacking into the computer systems of Internet users and posting their passwords on a public Web site. Their sentence was for 8 to 15 months. The prevalence of hacking confirms the need for a duty of security and confidentiality to protect a person's right to privacy. Nevertheless, there are conditions under which the duty is not binding, as the following case suggests.

In April 1999 the Singapore service provider SingTel, without informing its subscribers, scanned all of its 200,000 subscribers' transactions for a period of time while they were connected online. The company was looking for indications of hacking or other abuses. This, of course, was a violation of the subscriber's right to privacy, and a law student who discovered that her computer had been hacked by the Home Affairs Ministry reported the matter to the police. Public pressure ensued, and SingTel issued an islandwide public apology. Although this act was considered to be a breach of privacy, it was not deemed to be a crime as was hacking, however, because hacking was perceived to constitute such a threat to the Singaporean society. Learning from SingTel's experience, a Malaysian server provider called Jaring undertook the very same scanning procedures in September 1999. But Jaring issued notices warning all of its subscribers of its actions. Consequently, no public pressure or sanctions materialized. These providers were attempting to discover and thwart potential Maxims. Thus, when the common good is at stake, privacy can be sacrificed if it is done under proper, legitimate conditions. But a privacy/common good trade-off can only be made when people fully appreciate what their rights, duties, and exposures are with respect to their privacy.

This problem needs to be addressed on two fronts. First is the national and global policy front. Recent FTC and Gore-Clinton proposals and the financial

service bills currently being debated in the U.S. Congress are first steps. High on the list of requirements is the need for all decision structures to provide a high level of security for personal information and to restrict the flow of this information to just those subunits of the structure that have an agreed-upon relationship with the subject—that is, make each subunit a privacy capsule, in effect, a Rapp-type store. In particular, unauthorized parties, such as callers who misrepresent their true identity or employ other ruses (or bribes) to induce structures to disclose confidential information, must be thwarted and, if apprehended, punished. Second, and probably most important, we need to educate the citizens of this information society about the importance of managing information about themselves. In a liberal democratic society, citizens must be free to make decisions and act with a minimum of external interference. They must be able to create their own identity and sense of personhood. That is, they must enjoy liberty in both the negative and positive senses. But the price for this liberty is knowledge and vigilance. This burden falls on each of us and on our educational systems. People must know about the decision structures with which they interact and how these structures might use the information they acquire. People must learn how to enter mutually beneficial relationships with them, what to demand in terms of privacy safeguards, and how to monitor their performance. In short, we need to learn to build digital trust.

This point of view admittedly carries a Western bias. In nations where collectivism is more the norm than individualism, the unauthorized use of personal data is not seen as such an egregious violation of individual rights. In these societies it is a common practice to give out substantial amounts of personal information without question, not only during transactions with business and government but also during the conduct of other activities such as lucky draw lotteries, raffles, or filling out applications forms. Regarding themselves as interdependent rather than independent, members of these cultures do not view personal data as private. In fact, Singapore has a Statistics Act that requires organizations and individuals alike to provide considerable personal information. Failure to do so is a crime. Scandinavian counties such as Sweden have similar philosophies.

Not all Asian sites follow in Singapore's steps, however. In Hong Kong, Stephan Lau Ka-men, who previously worked for Citibank, EDS, and the Hong Kong government, has served as privacy commissioner for personal data since 1995. Under his leadership Hong Kong is implementing the Personal Data Privacy Ordinance, based on the Organization of Economic

Cooperation and Development's guidelines. These guidelines require individuals, public entities, and private companies to disclose their information collection practices. Similar to the fair information practices doctrine in the United States, the rules allow consumers to opt out of disclosing personal data, to have access to their records, and to be able to correct any errors. In addition, companies are not to collect data for one stated purpose and then use it for another.

In the unregulated, global world of the World Wide Web, one's privacy can be violated by irresponsible individuals as well as by well-meaning sellers of goods and services or menaces such as Maxim. In Singapore, for example, two students posted candid-camera-style unauthorized photographs of several young females on a provocative Web site that featured a chat room and articles on gender relations. They intended to make money through sponsorship and advertising. But as a result of many complaints, SingTel, the Internet service provider, removed the site from its servers. So the students moved their site to another host. Meanwhile, a debate ensued as to whether this act should be regarded as a criminal offence or a civil wrong. One Singapore lawyer claimed that publishing a photograph of someone without his consent is not, by itself, a criminal offense or a civil wrong. But using the photographs without permission to advertise or endorse a product or service, he argued, may be construed as defamation of character.

All of this points out a significant difference between Lucy's and Earl's businesses. Earl's was restrictively and comfortably local, whereas Lucy's and CD Universe's is inherently and inevitably global. Their privacy policies and protections must address a considerable number of differing cultures. They must strive for universality.

So far, with respect to consumer privacy, the asynchronous principle is applicable. Lucy and hordes of other Internet entrepreneurs, abetted by an exponential growth in technological capacity, are moving rapidly into the land of personal data use while society struggles to keep up its understanding of the meaning of these advances. In a market economy, the implicit assumption is that whatever brings economic success and satisfies customer demands is ipso facto good. But that isn't always true, and consequently, because little public debate on the legitimate limits of privacy and its appropriate safeguards has taken place, ethical reflection is lagging behind technological innovation. Systems that may materially affect people's lives are being implemented without thoughtful guidance as to whether or not they are leading us to the good society.

ORGANIZATIONAL AND POLICY SOLUTIONS

At the policy level, privacy may be protected by implementing a set of practices know as *fair information principles.* These principles derive from a moral understanding of informed consent as requiring the autonomous authorization of a data subject before a decision structure is permitted to acquire personal information. In 1973 the U.S. Department of Health, Education, and Welfare issued a code indicating what these principles might be. Among its provisions, which are applicable today, are the following:

- There shall be no personal data record-keeping systems whose very existence is secret. (Notice)
- There must be a way for a person to find out what information about the person is in a record and how it is used. (Choice)
- There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent. (Access)
- There must be a way for a person to correct or amend a record of identifiable information about the person. (Correction)
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data. (Data stewardship)[29]

In *Managing Privacy,* H. Jeff Smith suggests that the following provisions be added:

- There should be no deception in data collections practices.
- On a regular basis, a person should be given opportunity to opt out of any information practices he or she finds inappropriate.
- Within any organization that uses personal data, only individuals with a legitimate need to know—narrowly interpreted—should have access to the data.
- Disparate data files should not be combined unless the above provisions regarding clear description of purpose and opportunity to opt out have been met.
- Decisions about use of the data should be made through appropriate judgmental processes. Although many of these decisions can be made through automated processes, exceptional situations should be subjected to human scrutiny.[30]

These fair information practices are global ethical standards that tend to balance the needs of decision structures to have personal information with people's privacy concerns. They are procedures that provide individuals with control over the disclosure and subsequent use of their information. They also assure individuals that organizations will protect their personal information from the Maxims of the world. These principles are reflected in existing U.S. privacy laws, the European Union's directive on data protection, and other national laws such as the one adopted by Singapore.

At the heart of fair information practices are the following principles: notice, choice, access, correction, data stewardship, and redress/enforcement. People should be told what personal information will be collected and how it will be used. They should be given the opportunity to object if their information is to be used for purposes other than the original reason it was collected. People should be able to see the information the organization has collected about them and to correct errors. Organizations should ensure the security and the integrity of personal information. Finally, there should be means to ensure that organizations' practices are consistent with their policies and that there are procedures in place to provide redress in the event of problems. Fair information practices, therefore, mediate privacy concerns because they empower consumers with control and voice, even when the procedures are not invoked. They also provide an assurance that organizations will adhere to a set of principles that most consumers find acceptable. When a privacy horror story, such as some of those reported previously, appears in the press, it is usually a result of an organization's failure to adhere to one or more of these principles.

There is an emerging global consensus that fair information practices are the means to address the privacy issue. A consensus does not exist, however, as to how this should be accomplished. In the 1997 *Framework for Global Electronic Commerce,* the Clinton administration recognized that ensuring consumer privacy was essential if electronic commerce was to realize its full potential. Its section on privacy concluded with the following statement: "The Administration considers data protection critically important. We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy."[31]

Attempts have been made at self-regulation within industry. One such effort is the Individual Reference Services Group (IRSG). This group of organizations developed a set of industry principles governing the collection, use, and distribution of personally identifiable information that is applicable to the

use of any databases that reference or locate individuals. The FTC acknowledges that the IRSG's approach is "acceptable" and has indicated to Congress that legislation regulating the use of these individual information products and services may not be needed.

The recent FTC and Georgetown surveys of Internet privacy policies indicate, however, that voluntary implementation of fair information practices remains the exception rather than the norm on the Internet. As a result, there is increased interest in Congress for developing legislative solutions that would require organizations to disclose their information practices to consumers and to offer choice when information is to be used subsequently for unrelated or previously undisclosed purposes. The highly publicized denial-of-service attacks on popular Internet sites such as Yahoo! and eBay discussed earlier have raised awareness about the need for all systems connected to the Internet to implement appropriate security. However, the global reach of the Internet means that most laws will be difficult to enforce unless organizations are committed to fair information practices. Addressing the privacy problem consequently will require efforts by both business and government.

To build consumer trust, companies need to implement a privacy policy based on fair information practices. However, implementing a privacy policy is the bare minimum. Companies also need to develop a culture of privacy; that is, they must create an organizational culture in which, as Kant admonished, respect for people as ends rather than means is a core value and respect for their privacy is paramount. Developing a culture of privacy requires that privacy have a champion within the organization and that training and retraining employees to protect privacy is at the top of everyone's mind. Ideally, periodic internal audits are conducted to ensure that the company complies with its own privacy policy. Most importantly, a company must make concerns for privacy an integral part of the business case for every new use of personal information proposed.

◆ CONCLUSION

The provocations and trends mentioned at the outset capture this chapter's themes; the cases illustrate them. Earl was trustworthy with personal information precisely because he was a good person with very limited technological capacity. CD Universe attempted to be trustworthy, it appears, but the company lacked the dedication to security needed to adequately discharge its duties. Lucy is so wrapped up with technological optimism and greed that she may fail to even consider the ethical implications of her technologically based actions. These are contemporary scenarios. CyberHome.com, a possible 2010

business, will have as much as 120 times more computing and communication power available to it as today's organizations do. Moreover, information about people will be even more valuable circa 2010 than it is circa 2000. Consequently, CyberHome.com and its compatriot digital companies will be faced with an almost overpowering temptation to use the extensive, low-cost personal information they will have at their disposal. Privacy will be at risk.

The asynchronous principle predicts that the gap between technological capability and our ethical management of it and its prowess will widen even further in the years to come. We can close the gap only by starting to think deeply now about these possibilities and to develop the values, plans, and strategies society needs to ensure the health of that very precious aspect of the human condition: personal privacy. The policies discussed under the general heading of fair information practices are a good place to begin this reflection. Without this reflection, ethics will remain the caboose.

Notes

1. Ray Kurzweil, *The Age of Spiritual Machines: When Computers Exceed Human Intelligence* (New York: Penguin, 1999), 277.
2. *Computer Industry Almanac,* Dallas, TX: 1999.
3. Jeffery Rothfeder, *Privacy for Sale* (New York: Simon & Schuster, 1992), p. 23.
4. Richard T. De George, "Business Ethics and the Information Age," Center for Business Ethics, Bentley College, p. 3.
5. Scott McNealy, "Growing Competibility Issue: Computers and User Privacy," *The New York Times,* March 4, 1999, p. A17.
6. Amitai Etzioni, *The Limits of Privacy* (New York: Basic Books, 1999), 2.
7. This case is reported by John Markoff, "An On-line Extortion Plot Results in Release of Credit Card Data," *The New York Times,* January 10, 2000, pp. A1 and A6.
8. See www.cduniverse.com/asp/privacy.

8a. Tolkein, J.R.R., *The Lord of the Rings,* (New York, NY: Ballentine Books, 1991): 37.

9. Markoff, "An Online Extortion Plot," pp. A1 and A16.
10. S. B. Flexner, *The Random House Dictionary of the English Language,* 2d ed. (New York: Random House, 1987), p. 1159.
11. Samuel Warren and Louis Brandeis, "The Right to Privacy," 4 *Harvard Law Review,* 193.
12. Alan F. Westin, *Privacy and Freedom* (New York: Athenaeum, 1967).
13. Etzioni, *The Limits of Privacy.*
14. See John Markoff, "The Strength of the Internet Proves to Be Its Weakness," *The New York Times,* February 10, 2000, p. C1.
15. See, for example, Berlin Isaiah, "Two Concepts of Liberty," in *The Proper Study of Mankind* (New York: Farrar, Straus, and Giroux, 1998), pp. 191–242.
16. Kenneth Laudon, "Markets and Privacy," in *Computerization and Controversy,* ed. Rob Kling (San Diego: Academic Press), 705.
17. James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, MA: Harvard University Press).
18. James C. Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed* (New Haven: Yale University Press).
19. Rothfeder, *Privacy for Sale,* p. 23.

19a. (Moore's Law: A prediction made in the 1960s by Gordon Moore, cofounder of

Intel, that the number of transistors that could be put on a single silicon chip would double every 18 months.) See J. C. Simon, Introduction to Information Systems, (New York, NY: John Wiley & Sons, 2001): 196.
20. Diana Kunde, "Digital Divide Plagues Workers," *The Dallas Morning News,* February 11, 2000.
21. Mary J. Culnan, "Protecting Privacy Online: Is Self-Regulation Working?" *Journal of Public Policy and Marketing,* 19(1), 2000: 20–26.
22. www.amazon.com/exec/obidos /subst. . .policy/privacy.html, January 6, 2000.
23. Winnie Hu, "To Settle a Case, Chase Vows No More Customer Data to Marketers," *The New York Times,* January 26, 2000, p. B1.
24. Jeri Clausing, "Report Rings Alarm Bells about Privacy on the Internet," *The New York Times,* February 7, 2000, p. C10.
25. "FTC Investigating Amazon Unit over Software That Tracks Web Use," *The Dallas Morning News,* February 9, 2000.
26. Caroline E. Mayer, "DoubleClick Is Probed on Data Collection," The Washington Post Online, February 17, 2000.
27. DoubleClick press releases, doubleclick.com/company_info/press_kit /pr00.02.17.htm, February 17, 2000.
28. Peter H. Lewis, "Forget Big Brother," *The New York Times,* March 19, 1998, p. D1.
29. Computer Professionals for Social Responsibility, *The CPSR Newsletter* 7, no. 4 (Fall 1989): 16.
30. Jeff H. Smith, *Managing Privacy* (Chapel Hill: University of North Carolina Press, 1994), 210.
31. William J. Clinton and Al Gore, "Framework for Global Electronic Commerce," July 1997, www.ecommerce.gov.