Chapter 3 Ethics in IT-Configured Societies

Chapter Outline

Scenarios

3.1 Google in China: “Don’t Be Evil”

3.2 Turing Doesn’t Need to Know

3.3 Turnitin Dot Com

Introduction: It-Configured Societies

Technology as the Instrumentation of Human Action

Cyborgs, Robots, and Humans

Three Features of It-Configured Activities

Global, Many-to-Many Scope

Distinctive Identity Conditions

Reproducibility

It-Configured Domains of Life

Virtuality, Avatars, and Role-Playing Games

Friendship and Social Networking

Education and Plagiarism Detection

Democracy and the Internet

What Is Democracy?

The Arguments

Is the Internet a Democratic Technology?

Conclusion

Study Questions

Scenarios

Scenario 3.1 Google in China: "Don't Be Evil"

The Google search engine was created in 1998 by Serge Brin and Larry Page. Even though it was not the first widely available Web search engine (Alta Vista, Webcrawler, and Lycos were all available in 1998), Google rapidly became the most popular. Although exact figures are controversial, at this writing many estimates put Google's market share of Web searches at well over 50 percent. [http://marketshare.hitslink.com/report.aspx?qprid=4]

There are probably many reasons for Google's continued success at attracting users. Its algorithms for searching are advanced, it has invested in massive resources to increase performance, and its simple, uncluttered interface was distinctive when it first began. In addition, some also credit Google's famous motto, "Don't be evil," as part of its attraction. That slogan may have gotten Google positive free publicity, but it has also made Google vulnerable to criticisms about its policies, some of which seem to contradict its mission statement: "To organize the world's information and make it universally accessible and usable."

The most intense criticisms of Google have centered on its filtering (some would say "censorship") of particular content in particular countries. For example, in Germany and France Google filters out anti-Semitic websites to comply with laws in those countries against hate speech. Perhaps the largest controversy was over Google's entry into China, where the government requires extensive filtering, including blocking references to Taiwan, Tibet, and the Tiananmen Square massacre. Both Yahoo and Microsoft, key competitors to Google, entered the Chinese market and also agreed to these restrictions. (They, however, do not trumpet the slogan "Don't be evil.")

Google responded to the criticism about filtering by pointing out that "Don't be evil" also requires "Don't be illegal"; Google strives to obey the laws of countries where it operates. The company maintains that even limited access to the Internet is inherently democratizing, and that Google, as a public company, owes a duty to its shareholders to pursue business opportunities in China, even if that requires doing filtering that many find objectionable.

Google has tried to anticipate other possible trouble in China. For example, Google does not provide e-mail, chat, and blogging services in China (services they provide elsewhere) because they want to avoid confrontation with Chinese officials who might demand access to information about users posting content that the officials might find objectionable. (Indeed, Google and other providers have been forced to hand over such information in the United States in the U.S. government's "war on terrorism.")

Has Google done anything wrong? Is there a significant (ethical) difference between filtering hate speech in Germany and filtering political speech in China? Is the slogan "Don't be evil" appropriate for a publicly owned company? If so, is Google living up to that slogan? If not, does that mean working for a profit requires being evil?

Scenario 3.2 Turing Doesn't Need to Know

Hypothetical Situation

Indira is using instant messaging to get an answer to a question about a piece of software. She is interacting with Hal, a representative of the company that developed and distributes the software. During the exchange of text messages, it occurs to Indira that Hal could be a human (that was her initial assumption) *or* a sophisticated computer program designed to answer user questions. As Indira and Hal continue their conversation, Indira contemplates how to diplomatically ask whether Hal is human or not. Before she figures out how to bring up the subject, Indira receives a message from Hal that reads, "I'm just curious, Indira, are you human?"

What difference does it make whether Hal is human or not?

Scenario 3.3 Turnitin Dot Com

Hypothetical Situation

Giorgio Genova is a professor at a large state university. For the past several years he has been teaching a large class with well over a hundred students. Although the readings and assignments change each semester, the course objectives and main ideas that Genova is trying to get across stay the same. Hence, although Genova varies the essay questions on the take-home exams, they have been similar each semester. Genova is a fairly popular teacher; he works hard at teaching in ways that are effective. He believes, as do many of his colleagues, that it is important to gain the trust of students so that they engage with the material, feel comfortable asking questions, and come to appreciate the value of what they are learning.

With each of the take-home essays this semester, Genova has noticed that there seems to be an uncanny similarity in the opinions that the students express and the way they express these opinions. He is worried that because he has now taught the course for several years, there may be papers available from students who took the course in the past. So, Genova decides to run the papers through turnitin.com, a widely used plagiarism detection system. Turnitin.com compares the papers to content on the Web and to a database of papers that the company has accumulated as faculty have turned them in for testing.

Has Genova done anything wrong? What are the likely effects of Genova's actions on his students? How will widespread use of plagiarism detection systems affect classroom environments? Student–teacher relationships? The university environment?

Introduction: IT-Configured Societies

The term "information society" is often used to refer to societies in which IT is a critical part of the infrastructure through which economic, political, and cultural life is constituted. Although IT does not "determine" information societies, the activities, institutions, and social arrangements of

these societies are configured with IT. IT shapes, and is shaped by, these societies.

This chapter is devoted to understanding the role of IT in such societies and especially IT's role in configuring ethical issues and shaping social values. This is a daunting task and the strategy we adopt here is to examine information societies from several different perspectives, each building on the previous. We begin with the idea that technology can be conceptualized as the instrumentation of human action. Second, we identify several features of IT that come into play when it instruments human action and configures societies. These features are: global, many-to-many scope; distinctive identity conditions (often referred to as anonymity); and reproducibility. Next, we examine domains of life that have been created by IT (virtual reality environments) or affected by IT (friendship) or are in the process of being reconfigured around IT (education). Finally, we consider democracy and democratic values in IT-configured societies.

Technology as the Instrumentation of Human Action

Human action is a central focus of ethics. As explained in the preceding chapter, moral theories often target actions and try to identify what it is that makes actions right or wrong, good or bad, admirable or despicable. Is it consequences? Is it the universalizability of the maxim of the action? To be sure, action is not the only focus of moral theories; theories of justice focus on the distribution of goods and opportunities; virtue theories focus on the characteristics of a good person; yet other theories explore attributions of responsibility or core values or rules. Nevertheless, human action is a good starting place for understanding the connection between technology and ethics generally, and IT and ethics in particular.

When human action is the focus of ethics, technology is best understood as "the instrumentation of human action." This makes the connection between ethics and technology seamless. In IT-configured societies, many (perhaps, most) of the actions of individuals and organizations are instrumented through IT; the instrumentation adds efficacy and makes a difference in

what individuals and organizations conceive of as their options and what they actually do.

When human beings act, they move their bodies and what they do is a function of their bodies and the world their bodies encounter. I can throw a ten-pound object only so high and then it falls; how high it goes and how fast it falls is a function of my musculature, the size and shape of the object, friction, and gravity. Most importantly, our bodily movements have effects on others; our movements may have immediate effects on others or they may set off long, causal chains that have remote but significant effects on others. We are, perhaps, most aware of how our actions are a function of our bodies and features of the material world when we are confronted with what we cannot do. We cannot fly, leap to the top of tall buildings, and see through things (like Superman).

Technology adds to—expands, enhances—the instrumentation of our bodies. When we act with artifacts in a world filled with technological systems, our bodily movements have different and often more powerful effects than when we act without technology. I flip a switch and an entire building is illuminated; I press the trigger on a gun, and a small projectile goes faster and with more force than any human arm could ever throw; I press buttons on a phone, make sounds, and my voice reaches the ears of someone thousands of miles away. Indeed, with technology we can each, effectively, be Superman—we fly *in airplanes*, we reach the top of extremely tall buildings *with elevators*, and we can see through objects *using x-ray and magnetic resonance imaging machines*.

Technology changes what individuals are able to do and what they, in fact, do. Of course, all instrumentation is not equal. Particular technologies instrument human activity in quite distinctive ways. Automobiles instrument mobility, industrial machinery instruments manufacturing processes, eyeglasses expand vision, and thermostats control the temperature in buildings.

This is not, however, all there is to it because technology doesn't just expand human capabilities; it constitutes forms of action that weren't possible or even conceivable without the technology. "Genetically modifying food" and "watching television" were not just impossible before

the development of gene theory and mass media, they were incomprehensible. It is the same for IT-instrumented actions. IT expands what individuals can do and constitutes actions that were inconceivable before the technology existed. “Sending spam,” “searching the Web” and “blogging’” were incomprehensible and impossible before the creation of the Internet.

IT instruments collective or organizational action as well as individual action. Consider the case of a business that uses an IT system to instrument the work of its employees. When a company installs a performance monitoring system on its computers, data about employee behavior is automatically generated and stored while employees work. Records—of speed, accuracy, length and content of phone calls, idle time of machines, websites visited—become a seamless part of work. IT is used here to instrument the work of employees, and the instrumentation has features that were not part of the prior instrumentation. Yes, employers have always monitored the work of their employees, but the IT instrumentation changes the features and extent of the monitoring.

Thinking about IT as the instrumentation of human action has two important advantages for ethical analysis. First, it keeps humans as the agents of actions, and second, it allows us to focus on the contribution of the instrumentation to the character of human actions. In other words, this conception of technology positions human beings as central to technological outcomes—humans are the actors—while at the same time recognizing that the use of technology powerfully shapes what humans can do and what they actually do. Technology instruments what is always *human* activity, and human activity may be in part constituted by technology.

Cyborgs, Robots, and Humans

Before using this concept of technology, we can explain it further by responding to some possible objections. The account may be criticized, first, for not acknowledging the “agency” of technology. STS scholars have used the notion of “agency” to explain the role of technology in society; they argue that technology has agency in the sense that it contributes to

what happens in the world. What individuals, organizations, and even nation–states do is a function of the technologies through which they are constituted. Technology has efficacy, the power to effect outcomes.

As a field, STS might be understood to have as one of its goals to draw attention to the power of technology, that is, to understand and explain how power is wielded through technology. To achieve this goal, STS theorists argue for the "agency" of technology. For example, in what is labeled "actor-network theory" (ANT), sociotechnical systems are represented as networks—networks of things and people. Each node in a network influences what happens. ANT makes the point that we shouldn't privilege the contribution of human actors to various outcomes, so the theory recommends that we refer to each node in the network as an "actant." There are human and nonhuman actants. For example, a computer program is an actant as is the human user of the program. They each behave and the interaction of their behaviors produces outcomes.

Network theorists are likely to criticize our account of technology as the instrumentation of human action on grounds that it privileges human actors and doesn't sufficiently acknowledge the contribution of technology. Our counter is that our account allows us to see both the contributions of humans and of technology, and to see them as intertwined but distinct. In identifying technology as the instrumentation of human action, we link technology and human activity tightly and inextricably. Our reasons for keeping humans as "the actors" in our conceptualization of technology reflects our concern about another set of issues and another possible line of criticism of the account.

Coming from a quite different direction, critics may think we are mistaken to keep IT (not just any technology but IT in particular) connected to human action because IT systems have the potential to become autonomous actors. These theorists see how independently computer programs, bots, and robots can function. They anticipate a future in which IT systems will function even more autonomously and to a point that humans will not be able to understand what IT systems are doing, let alone control them. Some of these scholars argue that bots and robots may in the future function so autonomously that we will be compelled to grant them the status of moral

agents. They will be “artificial” moral agents and we will be obligated to refrain from turning them off—because of their moral status.

The debate about the moral status of autonomous computer programs, bots, and robots is important and will likely continue. It is important as much for what it reveals about the nature of cognition, intelligence, and morality as it is about what will happen in the future. We have adopted the account of technology as the instrumentation of human action in part with an eye to this debate, and with the intention of keeping in view that human beings are always involved in technological endeavors. When programs, bots, and robots seem to behave autonomously, it is because humans have built and deployed them to do so. If these systems function more and more autonomously, it will be because humans have chosen (by action or inaction) to put such systems in operation. Our account presupposes that technology is sociotechnical; wherever there are artifacts, there are social practices, social arrangements, and social relationships. In other words (and connecting back to the view of technology being proposed here), bots and robots *are* instrumentations of human action.

Interestingly enough, both lines of criticism—that our account doesn’t sufficiently acknowledge the contribution of technology and that it keeps technology too tightly linked to human action—have a common thrust. They are both concerned to show that humans are not fully in control of what happens in the world. STS scholars are struck by the powerful way that technology constitutes the world we live in and contributes to outcomes. The autonomous moral agent theorists see that programs, bots, and robots are behaving more and more independently. In both cases, the concern is to show not just that technology is powerful but that humans are not fully in control and cannot be responsible for what happens. Both accounts seem, in this respect, to border on technological determinism; they seem, that is, to presume that technological development and technology’s role in society are uncontrollable or keep going without human intentional activity.

We adopt the account of technology as the instrumentation of human action as a strategy to keep the connection between technology and human activity in full view. Our view incorporates the idea that technology is always

“tethered” to human beings. Of course, everything that happens isn’t intended. Unintended consequences are common, and combinations of intentional activity by different people produce results that no single individual intended. Nevertheless, technology is human-made and it doesn’t come into being or get deployed without human activity. Human activity is required both for production and deployment.

So, although it may be true to say that bots and robots with increasingly greater independence are likely to develop in the future, it would be a mistake to leap to the conclusion that humans will be compelled to adopt or deploy these technologies. To adopt the inevitability of “artificial moral agents” is both to slip into technological determinism and also to presume that notions of responsibility and the need to hold humans responsible for what happens will not come into play in the future. Concerns about accountability are likely to influence the deployment (if not the development) of autonomous bots and robots, just as systems of accountability (product liability law, torts, and other legal concepts) have influenced the development of current technological systems.

One way to think through the issues here is to consider a somewhat different account of technology and its role in human activity. Some theorists have suggested that we should think of ourselves as “cyborgs,” that is, human–technology combinations. This idea is most salient when we think about technologies implanted in our bodies, for example, heart monitors, replacement joints, and mind-altering drugs. Here it seems that we (or at least some of us) are cyborgs. But why restrict cyborghood to implanted artifacts? We live our lives seamlessly and intimately intertwined with technology; our lives depend on energy, transportation, and sanitation systems. Could we live as we do, be who we are, without electricity, medicine, and industrial agriculture? Without these technologies, we couldn’t and wouldn’t think of ourselves and our lives in the way that we do now. Thus, our being cyborgs is as much about the technologies that surround us as about those implanted in or around our bodies.

The idea that we are cyborgs is not far from our idea about technology as the instrumentation of human action. On the one hand, the cyborg idea seems to hint at the human component not being fully in control because a

cyborg consists of "silicon and carbon." On the other hand, this raises a question about how to conceptualize the actions of a cyborg, especially given the centrality of agency, action, and intentionality to moral theory and moral notions. The issues here are quite fascinating.

A major challenge for morality in IT-configured societies is to develop adequate notions of responsibility, notions that hold individuals responsible for their actions, and hold those who design and deploy technologies responsible for their actions. What is clear in all of this is that whatever we think about technology—whether we use the cyborg metaphor, allow for artificial moral agents, or think of technology as the instrumentation of human action—ideas about responsibility must be taken into account.

Scenario 3.2 hints at the themes that we have just discussed. The scenario depicts what may happen as IT-configured societies increasingly adopt sophisticated programs to deal with clients and customers for interactive functions that in the past were performed by humans. We already experience situations of this kind when we send questions to websites, receive responses, and then wonder whether the response was machine generated or a human being actually read our question and customized the answer. Of course, we can question the question: What difference does it make whether the client/customer is communicating with a human or not as long as the response to the question is adequate? Is it enough to say that humans simply prefer to know whether they are communicating with a person or not? Perhaps it should depend on the context. For example, some may feel more comfortable discussing medical questions with a person; they may believe that medical issues are so complicated, nuanced, and individualized that no machine could ever do as well as a person. There are also responsibility issues here. What if the answer given is inaccurate or misleading? Will accountability differ if a human gave the answer rather than a machine? Should we have a system of accountability in which a company is responsible for answers given, regardless of whether the answer was given by a human or machine agent?

We have explored two possible criticisms of our account of technology as the instrumentation of human action in order to draw out some of its implications. Because we will continue to use this account both throughout

this chapter and in subsequent chapters, the "proof" of its value will be "in the pudding" so to speak. The analyses we provide in the rest of the book will demonstrate the value of the account.

Three Features of IT-Configured Activities

In Chapter 1 we critiqued the standard account of computer ethics on grounds that it applies generally to new technologies and not specifically to computers or IT. The same could be said of our account of technology as the instrumentation of human action; it is an account of technology in general and although it applies to IT, it does not provide an account of what is distinctive about IT ethics. In this section we take on the task of identifying some of the distinguishing characteristics of IT systems. Although we are reluctant to generalize about IT because it is such a malleable technology, many of the ethical issues that arise in IT-configured societies seem to cluster around three features: (1) global, many-to-many scope; (2) distinctive identity conditions (in which individuals have the ability to be anonymous or pseudonymous); and (3) reproducible. For now, we will not be concerned with whether and how these features are produced; our concern is with their significance for ethical issues and their contribution to ethical dilemmas. We will begin by focusing on IT-instrumented communication, especially communication via the Internet, and will compare this form of communication with face-to-face, telephone, television, and radio communication. [Note that the comparison is a little convoluted because telephone, television, and radio are now thoroughly computerized and often instrumented through the Internet, although they were invented and functioned initially without computers.]

Global, Many-to-Many Scope

When we communicate without any form of technology, we have a fairly limited range. Whether we speak softly or yell at the top of our lungs, we can speak only to those who are geographically close. Our reach is limited by the structure of our throats and ears and how sound travels. Megaphones, telephones, and hearing aids expand the range of the spoken word. Writing makes use of technology, and the reach depends on the technology one uses

—pen and ink, typewriter, and so on. Once one puts words on paper, the paper can travel great distances by means of messengers, carrier pigeons, pony express, or extremely complex mail delivery systems, for example, the U.S. Postal Service and FedEx. The reach of individual communication has been significantly expanded through IT and the Internet. With relatively little effort, an individual can with very simple movements reach others who are on the other side of the earth.

Internet-instrumented communication has a global scope. To be sure, the Internet does not allow us to communicate everywhere, and to everyone in the world, only with those who live in places where there is electricity, computers, and other technologies that receive telephone or satellite signals. Still, even with this limitation, the Internet significantly expands the scope of individual and organizational reach, and the expansion is especially significant in relation to the effort involved. That is, with the proper equipment and service, individuals achieve this expanded scope with relatively little effort.

Although the expanded scope of communication on the Internet seems enormous when we compare it to face-to-face communication, it is not so enormous when compared to the mail services, telephone, or radio and television transmission because these also have global reach. Oddly, the system with the largest scope seems to be hard mail (sometimes derided as "snail mail") because it does not depend on electricity as do telephone, radio, television, and the Internet. Letters sent via hard mail can reach many more places than the Internet. The comparison is interesting because it suggests that the importance of the global scope of the Internet is tied to its ease of use, immediacy, and low cost. We can write on paper and send our paper messages via a postal service, or we can publish our written words in a newspaper, magazine, or book that is distributed around the world. However, by comparison with the Internet, these forms of communication are cumbersome, expensive, and slow. Writing messages on paper—even if we duplicate the same message for thousands of people—takes more time and energy than moving our fingers over a keyboard and clicking on icons. Getting something published in a newspaper or magazine is quite complex and fraught with uncertainty. So, the significance of the global scope of the Internet is a function of ease, immediacy, and affordability.

Television and radio communication are similar to the Internet in global scope and immediacy. One simply speaks into a microphone and the words can reach huge numbers of people. The important difference here is that radio and television communication are one-way from station to listeners and viewers. We can refer to this as one-to-many communication to contrast it with the Internet's capacity for many-to-many communication.

It is tempting to characterize the Internet's many-to-many scope as distinctively interactive, but we have to remember that face-to-face communication is highly interactive. So, it is not interactivity alone that is the unusual feature of communication via the Internet. Nor is it ease alone or global reach alone. Rather, it is the combination of elements we have just discussed. The Internet provides to many individuals who are geographically distant from one another the capacity to communicate easily, quickly, and cheaply. It provides something to individuals that was, before the Internet, available only to a few—namely those who owned, or had access to, radio or television stations or could afford long-distance telephone calls. The Internet puts this instrumentation in the hands of many, allowing many to communicate globally with many others.

Distinctive Identity Conditions

Although it is tempting to say that anonymity is a distinctive feature of communication on the Internet, this is not quite accurate. For one thing, our communications on the Internet are monitored by service providers and can be traced by other interested parties, those who have a legal right to access the information or who have the technology that allows them to (illegally) access it (e.g., with packet sniffers). The temptation to think of Internet communication as anonymous seems to arise from the fact that we do not see each other directly when we communicate on the Internet. A famous *New Yorker* cartoon captured this idea as it depicted a dog in front of a computer thinking, "no one knows you're a dog on the Internet."

A more accurate characterization would be that communication on the Internet is mediated. A complex sociotechnical system instruments what we say to one another online. Typically, we cannot see each other directly, that is, we don't have access to visual cues about one another when we

communicate via e-mail, chat, or use instant messaging. However, Web cams and other new technologies are likely to become more common, so this may change. In any case, mediation means, among other things, that there is always the possibility of intentional or unintentional distortions of identity, for example, machine-generated images that disguise the person. Humans have relied on their senses to determine the identity of others for thousands and thousands of years, and because of this, the trustworthiness or reliability of our identity in electronic communication may always be an issue, if for no other reason than that technology can be manipulated more easily than a physical presence.

The claim that Internet communication is unique because it affords anonymity is also problematic because anonymity is itself a complex concept. Anonymity seems to be contextual and relational. One can be anonymous to one person while identified to another. We can do a variety of things to make our identity more or less apparent to particular individuals. For example, you can use an e-mail address that hides your real name. You can use pseudonyms in chat rooms and virtual games. You could even have several Facebook identities, making some information available under one identity and other information available under another.

To illustrate how complicated anonymity is, consider the following situation. I get in my car and drive several hundred miles away from my home. I stop my car, enter a grocery store, and buy groceries, paying with cash. I could be said to be anonymous in this grocery store because no one in the store knows me or pays much attention to me. No one knows my name, what kind of work I do, where I live, how I feel, and so on. Oddly, while I was anonymous in these ways, I was in full view. People in the store, if they had bothered to notice, could see what I looked like, what I was wearing, and could have gauged my weight, height, age, and so on. The anonymity I had in this situation seems to have something to do with the fact that no one in the store knew my name, or could connect the information available to them (by looking), with any other information about me, for example, my address, occupation, or political affiliation.

The kind and degree of anonymity one has in any situation seems to depend on the ways in which, and extent to which, information can be linked with

other information. To see this, consider one change in the situation just described. Suppose that I make a purchase at the store but use a credit card instead of paying in cash. My behavior is now instrumented through a vast and complex technological system that involves information moving from the store to a credit card company that is linked to other institutions through which I pay my credit card bill, for example, my bank and a credit rating agency. Each node in this vast financial system has information about me. Thus, once I use my credit card, my identity condition in the store has changed. If later in the day a crime is committed in the area, the police might ask whether anyone in the store noticed strangers, and if someone has noticed me, the police can ask the store to go through their transaction records, and pull my credit card information. With my credit card number, it is easy for the police to obtain a wide array of additional information about me.

Now consider a different situation. When I go to the polls to vote in a local, state, or national election, I am required to provide a form of identification that includes my name and address (to verify that I am a qualified voter). I am also required to sign the register, attesting to the fact that I am who I claim I am. I proceed to the voting machines—assume here a mechanical-lever voting machine—and cast my vote on a machine that is entirely disconnected from the book containing my name, address, and signature. My vote is anonymous in the sense that how I voted cannot be connected to me (my name, address, signature). Remember, however, that my vote was recorded—it was counted. So, whereas *how* I voted was anonymous, *that* I voted and *where* I voted is not. Here, once again, linking of information is important in the sense that the system is designed so that a link cannot be made between me and how I voted. Yet, I was not exactly anonymous insofar as there is a record of my having signed in, a record connected to my name and address. [Note that the disconnection between an individual and his or her vote is still meant to be maintained with electronic voting machines. The problem with electronic voting machines is that individuals are increasingly unsure that their vote is actually being counted.]

So, anonymity is complicated and its role in various activities is contextual. Anonymity depends on certain things being known or not known by particular others in particular contexts. Complexity aside, it should be clear

that anonymity involves minimizing the kind of links that can be made to different kinds of information. In the voting case, my name and address are known but this information cannot be linked with how I voted; in the grocery store case, information about my appearance and location are known, and as long as I pay in cash this information isn't linked to other information but if I pay with a credit card, links can be made.

So, it isn't accurate to say simply that anonymity is a feature of communication on the Internet. Nor is it accurate to say that pseudonymity is a unique feature, because pseudonymity is possible in face-to-face communication and telephone communication. Individuals can disguise themselves by wearing masks and distorting their voices, or they can simply tell lies about who they are and what they want.

Perhaps the best way to characterize these aspects of Internet-instrumented communication is to say that there are distinctive identity conditions in Internet communication. The distinctiveness comes from two elements: (1) mediation—Internet communication is mediated through a vast sociotechnical system, and (2) the range of identity conditions that are available.

As already noted above, when we communicate via the Internet, those with whom we communicate do not see us directly; they see traces of us, traces that are produced in IT. Although many of us have become quite accustomed to this, it differs from the traditional mode of communication in which we use information about physical appearance (what people look like, what their voices sound like, and how they move their bodies) to identify others. Traditionally, humans have relied on this kind of information especially for continuity, that is, to know when we encounter someone we have encountered before. A person's physical appearance, voice, and facial expressions are used to fill in our understanding of one another as whole persons. The fact that the Internet does not give us this information is part of the difference between online and offline identity conditions. It seems to make some users "feel" anonymous but the feeling, as the preceding analysis suggests, may be quite misleading.

The second distinctive aspect of identity conditions in Internet communication is variability. IT instrumentation makes a variety of formats

possible and these formats, in turn, facilitate and constrain identity conditions. In virtual games, we communicate through our characters (avatars); in chat rooms or social networking sites, we can, if we choose, adopt pseudonyms and remain somewhat anonymous or we can provide accurate, detailed information that is easily linked to other aspects of our identities. This array of possibilities for identity seems distinctive, and important.

One final caveat is necessary. When it comes to identity and the Internet, there is always a gap between persons and machines. Tracking and monitoring of online communication involves watching machine activity, and thus, there is almost always a question about who produced the machine activity. In Chapter 6, where we take up IT-instrumented crime, for example, we will see that even when criminal behavior is traced to a machine located in a particular place, there is still a problem in determining who was controlling the machine when the machine was used in a particular way.

Reproducibility

A third important feature of Internet communication (and IT in general) is reproducibility. Electronic information is easy to copy and there is generally no loss of quality or value in the reproduction. Moreover, because the original is left intact in the process of copying, there may be no evidence that electronic information was copied. This feature has dramatic implications for property rights and crime. When physical objects are stolen, the object is gone and the owner no longer has access. When electronic information—be it a record, a program, or a piece of proprietary software—is copied, the original is still there, the owner still has access, and there may be no indication that a copy was made.

Reproducibility is a significant aspect of Internet communication because of what it allows. When you utter words in unrecorded face-to-face communication, the listener hears the words, and then they are gone. This is not the case with Internet communication. The words endure. They endure in the sense that they exist in machines and remain there unless and until they are deleted. Indeed, deleting words exchanged in Internet

communication can be no small feat. You may delete a message from your outbox, but the person who received the message may keep the message and may forward it to others who copy it and send it to yet others, and so on. As well, your service provider may maintain records of your communication.

In a sense, reproducibility expands the scope of IT-instrumented communication in time and place, but this expansion of scope means less control of written words by those who write them. The gain and loss seem to go together. Depending on how, and to whom, you send your "words," they may exist forever in someone else's machine. In a sense, endurance is the default position in Internet communication because if you do nothing, your communications continue to be available; at least until service providers delete them.

Reproducibility also expands the possibilities for disconnection between words and people. It makes it possible for one person to copy the words of another and then change them, or keep the words the same but use them as if they were their own. For example, the reproducibility of information on the Web has made it possible for individuals to copy information and claim it to be theirs, or to change the words of others so that someone else is misrepresented. This reproducibility is sometimes referred to as making possible "cut and paste" environments. [We will discuss the implications of this "cut and paste" capacity in education in a moment.]

So, these three characteristics—global many-to-many scope, distinctive identity conditions, and reproducibility—seem to distinguish IT-instrumented communication. To be sure, online systems can be designed so as to limit the scope of communication, make identity conditions similar to those offline, and prevent reproducibility, but more often than not they are features of activities in IT-configured societies. Geographic distance becomes less and less essential for everyday life and global interaction more and more common; individuals and organizations construct identities and pseudo identities online; and information gets reproduced effortlessly over and over again. In the remainder of this chapter we will see precisely how these characteristics come into play in many domains of life. In Chapters 4 and 5, we examine how they shape privacy and property rights

issues, and in Chapter 6, we explore how they affect crime and security, and other issues of law and order on the Internet.

IT-Configured Domains of Life

To explore the implications of these three characteristics for ethical and value issues in IT-configured societies, we will briefly examine three domains of life in which IT plays a prominent role. Our aim here is to illustrate the ethical challenges and changes that occur when activities are constituted with IT.

Virtuality, Avatars, and Role-Playing Games

One of the most fascinating aspects of living in an IT-configured world is the opportunities for participation in virtual environments. Role-playing games are one such environment. In these games, players interact with one another in real time through avatars—characters created by players using the gaming software. Avatars are software constructions manifested graphically and textually. Players are able to control their avatars through a keyboard; they are able to have the avatar move and speak in ways that are unique to each game. Avatars interact with one another in worlds with qualities unlike those of the natural world. The virtual rape case described in Scenario 1.1 took place in one of the first virtual reality game sites. LambdaMOO still exists but many more sites are now available including EVE online, Everquest, and Second Life.

Although it is possible to limit access, many virtual games have global, many-to-many scope. Through their avatars, individual players interact with other players who may be anywhere in the world. However, of the three features discussed above, the identity conditions of interaction in virtual games are the most interesting because they are what make for "virtuality." In virtual environments, players experience other players through their avatars. No one playing the game may know the offline identity of any other players and they don't acquire information that is linkable with other information about the person. In this sense, players are anonymous and they are also pseudonymous insofar as their identity is in their avatar. Avatars can exist over extended periods of time and have ongoing relationships with

other avatars. Players may not intend that their avatars be their "representatives"; that is, what players do outside the game and what they have their avatars do are understood to be different. Avatars are an opportunity for players to explore different identities and experience what it is like to be a particular kind of being. Nevertheless, avatars are expressions of their controllers.

Although the virtual rape case described in Scenario 1.1 took place many years ago, it continues to be useful for exploring the ethical challenges of virtual environments. The incident occurred at a time when little attention had been given to the status or meaning of avatar behavior or the attachment relationship that seems to form between player and avatar. When the virtual rape case first came to the attention of computer ethicists, the case seemed to comfortably fit the standard account. Individuals had new possibilities—manipulating avatars of their own creation in virtual games—and there was a conceptual muddle and a policy vacuum with regard to the new form of action. How could and should we think about the behavior of Bungle and/or the behavior of the person controlling Bungle? Because participants in the game expressed distress and anger about the so-called rape, what were we to make of the fact that no "real" rape had occurred? Had anyone done anything wrong? Who was wronged? What harm was done? Who and how might someone be punished?

Initially, it seemed that we might try to separate out what happened in the virtual environment from the people who were controlling the avatars. For example, it would be easy to say that because it was all virtual, any punishment or consequences should also be virtual. Punish Bungle and leave it at that. Of course, it is unclear what would be involved in punishing Bungle. Would we simply enact a virtual punishment? Put Bungle in a virtual jail for a given number of years? The problem with this approach is that the individuals who were upset and distressed about the virtual rape were the flesh-and-blood controllers of avatars. So the case cannot be dismissed so easily. To treat the wrongdoing as merely virtual and respond only within the virtual room doesn't acknowledge that virtual worlds are also "real" in important respects.

When the case first came to the attention of computer ethicists, it seemed a good candidate for analogical thinking. We might think of behavior in virtual environments as a form of expression like writing a story or making a movie. Written words and images can be harmful, as in pornography and violent films, and especially when individuals are exposed to these visual and textual forms without their consent or when they are under age. Offline, we hold individuals legally and morally responsible for exposing children to pornography and even with adults, we require that they be given warning so they have the opportunity to avoid exposure. For example, bookstores selling pornography are not allowed to display their goods as part of their advertisements; they must forewarn customers about their wares. If the wrongdoing in the virtual rape was that of exposing members to pornography and violence without warning, then clearly the wrongdoing was that of the person controlling Bungle, not Bungle. Of course, the person controlling Bungle didn't rape anyone. Because rape is one of the most serious crimes committed against human beings, it seems misleading and somewhat disingenuous to even refer to the case as a rape. Rather, Bungle's controller, it would seem, harmed the other human players by exposing them to a level of violence that they did not expect or want to see in LambdaMOO.

This preliminary analysis has the advantage of framing the game—LambdaMOO—as a sociotechnical system. The game consists of software and hardware, people interacting through and with the software, and people with ideas about what they were doing and how they should behave. The software allows players to engage in certain kinds of behavior and prevents them from engaging in other kinds. Whether aware of it or not, the players had ideas about what they were doing, and those ideas shaped the game—the virtual world. Implicitly, most players adhered to social norms of behavior similar to those they might adhere to offline. They maintained certain rules of civility. The person controlling Bungle had a different idea. He broke the norms of civility assumed by other players. Today, most role-playing games specify norms for the game through rules and contracts, and players must explicitly commit to these before they join the game.

Notice that the social norms of the game were not just in the minds of the players, they were also in the software. The game software was set up so

that no one but the game wizard (administrator) could control certain aspects of the game. As well, the software had been set up so that each player could control his or her own avatar. Bungle's controller didn't just violate a norm with regard to the level of violence in the game, he or she gained unauthorized access to the system and took control of the characters that had been created by other participants. Thus, Bungle's controller violated the social *and* technological norms of the game, that is, norms embedded in the software and in the thinking and behavior of other players. The virtual rape case is, then, a good illustration of the sociotechnical aspects of morality. Moral norms can be socially and technologically constructed.

This analysis of the virtual rape is far from complete; the LambdaMOO incident continues to peak the interests of computer ethicists, and the most recent literature suggests that in analyzing role-playing games, one has to come to grips with the attachment that individuals form with their avatars. As one scholar recently explained, avatars are "the embodied conception of the participant's self through which she communicates with others in the community" (Wolfendale, 2007). The attachment relationship is important because it provides a basis for understanding why many players felt that they had been wronged or harmed by Bungle's behavior. Remember that Bungle's controller had to take control of avatars that belonged to others in order to perform the rape. We can imagine that the legitimate controllers of legba and Starspinner were angry both because their control had been taken away and because "their" avatars had been used to enact a rape. We might even say here that legba and Starspinner were demeaned and disrespected in the rape enactment, and, therefore, their creators were demeaned and disrespected. When players identify with their avatars, they have strong feelings about how the avatars are treated.

So, another way to think about the wrong done in the virtual rape case is to frame the actions of Bungle's controller as harming the other players by showing disrespect for avatars understood as expressions to which individuals were strongly attached. Although not definitive, an analogy might be helpful here. The attachment of a player to his or her avatar might be seen as analogous to a person's attachment to his or her family emblem or memorabilia of a favorite sports team. If someone were to spit on or step

on your family emblem or the shirt of your favorite soccer player, you might well be offended. You might take this to be a serious personal assault.

We do not claim that any of these accounts of the virtual rape case are the final word. Virtuality is complex and its meaning is far from settled. What is clear is that IT has configured a form of interaction that is shaping, and being shaped by, several factors including moral norms and practices. Issues of this kind are likely to continue to arise as IT-configured societies evolve.

Friendship and Social Networking

In IT-configured societies, friendship is instrumented, in part at least, through a variety of IT systems including social networking sites, chat rooms, instant messaging, e-mail, cell phones, text messaging, and more. These technologies affect who your friends are, how much contact you have, when you have contact, what and how much you know about each other, and what you say and do together. In this respect, modern friendship is a sociotechnical system.

That friendship is taken up in a book on ethics may seem odd to some, but friendship has been a topic in moral philosophy going back to the ancient Greeks. Aristotle's analysis of friendship continues to be used by contemporary philosophers as the starting place for thinking about friendship, what it is, and why it is so valuable. Aristotle gave an account of friendship that may seem idealistic, although the fundamental ideas are relevant to friendship today. Aristotle believed that true friends cared about each other in a special way. Friends are those who you care about for their own sake. You care about them and their well being not because you may benefit from the friendship or because their good may somehow promote your good. Aristotle also believed that friendship achieved its highest value when friendships are based on an appreciation of the other's quality of mind and character. You choose friends because you respect their qualities and character, and the better those qualities, the better the friendship.

Friendship on the Internet has come under the scrutiny of computer ethicists, and some have questioned whether "true" friendships can be

formed online. Recent research has indicated that we may be using the Internet and IT not as much to initiate friendships but to supplement offline friendships with those who we also meet face-to-face. Nevertheless, critics have raised questions about the limitations of online communication and, therefore, online friendship. As an example of the critical perspective, consider that Dean Cocking and Steve Matthews (2000) published an article titled "Unreal Friends" in which they argued that real friendships could not be established or maintained on the Internet. Building their argument on the insight that communication is affected by contextual factors. Cocking and Matthews articulate a concern about the ways in which the Internet environment structures and constrains verbal behavior. They argue that the Internet environment distorts important aspects of a person's character (that is, it distorts what individuals reveal about their character) and weakens the interactions in which persons develop a relational self through their interactions with their friends. Their argument is based on recognition of a significant difference in the kinds and degree of control that individuals have over self-disclosure in online communication as compared to offline. Their argument is connected to Aristotle's idea that friendships are better when they are based on the qualities of a friend's character. If the Internet limits what one can learn about friends, then it limits the possibility of true friendship.

Whether or not we agree with Cocking and Matthews about the Internet constraining (or distorting) friendship, their claim that communication on the Internet differs from face-to-face communication seems right and so does their focus on what individuals reveal about themselves online. Moreover, the differences between online and offline relationships are not limited to differences in self-disclosure.

Historically, individuals have had close friendships primarily with those who lived in the same geographic area because living in the same location meant frequent contact, frequent opportunities for interaction, and shared experiences. Over time and long before IT, technologies expanded the scope of friendship, if not for creating, at least for maintaining relationships. Think of friendships maintained by letter writing and how that was affected by expansion of the mail system through railroads and airplanes. Think of friendships maintained through telephones and, of course, through

improvements in our capacities to travel. In the past, individuals lost touch with friends who moved away or if they didn't lose touch, communication was less frequent and this made it difficult to maintain intimacy. Social networking sites, cell phones, IM, and chat rooms have expanded the scope of friendship and increased the possibilities for frequent contact regardless of place and time zone. It doesn't matter nearly as much where your friends are, as long as they have access to the Internet and cell phone towers.

Although we shouldn't forget that individuals consciously construct their identities offline—in their choices of clothing, haircut, the car they drive, how they furnish their room or apartment—IT structures the construction of identity online. Think here of social networking sites and what the default settings have one reveal. We construct our identities as well when we make decisions about our user ID; what, if any, quotation we use in our e-mail signature; and the information and images we post on Facebook. Here we can see that the architecture of a system can make a difference in how one constructs one's identity and, in turn, the conception that friends have of us.

Reproducibility also plays an important role in Internet-instrumented friendship. Remember that in face-to-face interactions, words are spoken and then they are gone. Someone may with effort try to listen in on a face-to-face conversation but it takes a good deal of effort and technology to record what you say. Interactions with friends in IT forums are reproducible with little effort. Internet service providers often keep records and can make them available to law enforcement agencies (with or without a warrant). And, as we saw in Scenario 1.2, employers and law enforcement agencies examine information on social networking sites. As users become more aware of this, they may construct their identities differently.

It would seem, then, that friendship instrumented through IT differs from friendship instrumented through other technologies, but the significance of the differences is unclear, especially when we remember that what is at issue is not online versus offline. Most commonly, friendships are established and maintained online *and* offline. At the extreme ends of the continuum are friendships that exist only online or only offline, but in between are a wide range of hybrids. Some friendships begin online and

move offline; others begin offline and move online, and in either case, the amount of offline and online can vary widely and change over time.

In Chapter 4, we will focus on privacy and there we will see that the flow of information in relationships affects the nature of the relationship. We will then raise the question whether intimate relationships can develop in environments in which there is little or no privacy. That discussion will supplement our discussion of friendship in this chapter.

Education and Plagiarism Detection

Many aspects of education have been reconfigured around IT. Think of online application processes, communications between teachers and students, record keeping, and online courses. At the most profound level, the permeation of IT in education has disrupted ideas about the purposes, values, and measures of education; in other words, the reconfiguration of education around IT has changed ideas as to what it means to be educated. This transformation has happened not just because of the adoption of IT but also because IT is seen as the infrastructure of the future. Thus, educational institutions have embraced goals that have to do with preparing students for a life, jobs, and citizenship in a world filled with IT.

As an illustration of the subtle, but profound, changes in ethical norms and values that occur when education is instrumented with IT, consider plagiarism and plagiarism-detection systems. Of course, issues of academic integrity and plagiarism predate IT; teachers have long dealt with students who cheat, and plagiarism has long been defined (in the United States and many European countries at least) to include direct copying of text that has been written by someone else.

However, because of the reproducibility of information and the accessibility of information on the Internet, it is much easier to cut and paste text (segments or the whole of an assignment) and claim it as one's own. A slightly more sophisticated form of plagiarism is to cut and paste, manipulate the text slightly, and then claim it as your own. This is a case where one of the enormous benefits of IT and the Internet are butting up against the values of a domain of life. On the one hand, it is a boon that

information is so accessible, and the ability to cut and paste it makes it easy to keep and use. On the other hand, educational institutions have as goals that students master knowledge and demonstrate their mastery by producing that knowledge on their own, and that students learn to think and write and demonstrate their ability to do so by producing thought and expressing it in writing or verbally "on their own."

At the moment, we seem to be in the midst of a collision between what is possible and easy *and* the norms of education. At a deep and often not articulated level, educational goals and strategies are being challenged and rethought. Perhaps education has to change to accommodate to a world in which cut and paste is the norm. Perhaps the nature of writing is changing. Perhaps we need to rethink what and how we teach. On the other hand, it would seem that educational institutions must evaluate students and decide whether and when they have achieved certain levels of mastery. If "cutting and pasting" undermines their ability to do this, then institutions must have ways to identify and discourage illicit cutting and pasting.

The solution that many teachers have adopted is to use what are called "plagiarism detection systems." Turnitin is the most widely used system. Teachers submit student papers and Turnitin tests these papers in two ways: It checks the papers against published material and against unpublished material. In the latter case, papers are checked against a database of papers that the company has created from papers that have been turned in for testing. [This, by the way, has raised a number of legal issues about the copyright status of student papers.] The tester may find segments of a paper that are identical to published work or segments of text (or an entire paper) that are identical to a paper in its database.

It is worth noting here that Turnitin doesn't exactly find plagiarism; it finds matches between text; the matches may or may not mean plagiarism. A teacher has to review the matches and make a determination. For example, if a student quotes a paper, puts that text within quotation marks, and cites the source, then the student has not plagiarized at all. Turnitin doesn't distinguish that case from the case in which a student copies an entire paper without attribution. Thus, although it may seem a simple matter, systems

like Turnitin create a form of information that has to be interpreted as plagiarism.

A major issue here is the reliability of such systems. Concerns have been expressed that some plagiarized papers are not detected, that some nonplagiarized papers are identified as plagiarized, and that the results may be skewed against students for whom English is not their first language (Introna, unpublished). John Royce (2003) argues that the reliability of such systems can be demonstrated only when papers that are known to be plagiarized are submitted and caught. He cites four studies that used this approach but the results were mixed. In his own study, John Royce found that Turnitin "found no matches for material lifted from usenet discussion groups and discussion lists."

Reliability aside, there is an issue as to how automated plagiarism detection reconfigures values. Education depends in part on trust between students and teachers. Students have to trust that teachers will teach them what they need to know, and teachers have to trust that students will tell them when they understand something and when they don't. Student–teacher relationships are not unlike doctor–patient relationships in the sense that just as doctors cannot diagnose problems and identify appropriate treatments unless patients tell them about their symptoms, teachers cannot figure out what students don't know and how best to teach them unless students are honest in their responses to homework, research papers, and tests. In other words, if students hide their lack of ability and knowledge, they won't receive the education they need.

The problem with plagiarism detection devices is that they tend to create an environment of mistrust. When a teacher runs an entire set of papers through a plagiarism detector, the teacher is assuming that each and every student is a potential plagiarist. Even if the teacher selects only certain papers for submission to plagiarism detection, the teacher runs the risk of differentially bringing certain students under suspicion. Either way, if educational environments come to be based on mistrust, students will not develop maturity or the capacity for independent learning that is so critical to their futures. This is not an argument against the use of plagiarism detectors but rather for careful usage. Plagiarism detection systems are

sociotechnical systems, and attention ought to be paid to the social practices that constitute these systems. In particular, attention should be paid to how students and teachers are "constructed."

The reconfiguration of education around IT, like that of other domains of life, continues to evolve. Although it seems unlikely that plagiarism detection systems will go away, the technology and social practices of plagiarism detection have not yet stabilized; they are being worked out.

Democracy and the Internet

So far we have used several different approaches to understand the significance of configuring societies with IT—conceptualizing technology as the instrumentation of human action, identifying the significant features of IT, and examining three domains of life in which IT has an important role. We turn now to another important approach. Many computer enthusiasts, the popular media, and a number of scholars have suggested that IT and the Internet are "democratic technologies." The claim is intriguing because it seems to assert a form of technological determinism; that is, the claim seems to affirm that adoption of IT and the Internet will lead (necessarily) to the adoption of democratic practices and arrangements. If we think of democracy as a value, then, the claim is that IT somehow embodies democracy. To put this in a somewhat different way, if we think of democracy as a political form, the claim is that IT requires, necessitates, or at least facilitates democratic forms of social interaction.

So, what are we to make of the IT–democracy connection? Is IT inherently democratic? Will increasing use of the Internet lead to a more democratic world? If so, is there something about the hardware, software, and telecommunication lines—the artifactual components of the Internet—that leads to democratic social arrangements? Or is it that IT and the Internet are so malleable that they can be molded to fit democracy but could also be molded to fit nondemocratic arrangements? For example, the massive surveillance possibilities to be discussed in Chapter 4 could contribute to totalitarian control. In any case, these questions call upon us to think about democratic societies as sociotechnical systems, and then to examine the

contribution of the artifactual and social components to the achievement of democratic institutions and arrangements.

From the early days of computing, social theorists suggested that IT had an enormous effect on power relations. Initially, the issue arose because computers were so large and expensive that social observers presumed that the primary users would be large institutions—governments and corporations, and these users would become more powerful. In other words, computers would lead to more concentration and centralization of power. This perception and concern changed with the invention of micro-, or personal, computers. Smaller, less expensive machines meant that more people could have the enormous power of computers, and this meant decentralization of power.

Another factor contributing to the idea that IT is democratic is directly related to reproducibility. Many believed early on that because information and programs could be copied without any loss of content or quality, and at seemingly no cost, IT had the potential to revolutionize the availability of knowledge much as the printing press did in the fifteenth century. This contributed both to the idea that the technology would be revolutionary and to the idea that it would be democratic. Arguably, the open source movement is an extension of this idea because those in the open source software movement see it as a movement that will bring the benefits of IT to many more people. We will discuss this movement in more detail in Chapter 5.

What Is Democracy?

The claim that IT or the Internet is a democratic technology raises a prior question: What is democracy? Democracy is a complex idea probably best understood as a cluster of ideas, values, and arguments and, hence, characterizing a technology as democratic raises more questions than it answers. The core idea of democracy is, perhaps, best expressed as the idea that political power should reside in the citizens of a nation, rather than in a single person (a monarch or dictator) or small group of persons (an oligarchy or aristocracy). In democracies, citizens are the ultimate authority, and the government is accountable to those citizens. This idea has been

articulated and interpreted in a variety of ways, and reinterpreted and modified over time. In a sense, democracy has been embodied in somewhat different ways, at different times, and in different places. Consider the array of democracies that now exist around the world.

Democracy is a moral concept in the sense that it has an underlying moral justification. Democratic theory is built on the idea that individuals are sovereign over themselves, and to be recognized as such they must have some say in the governments by which they are ruled. This may seem Kantian because it recognizes citizens as ends in themselves, not merely as means to a monarch's or dictator's ends. Nevertheless, some democratic theorists have provided utilitarian justifications for democracy. John Stuart Mill, for example, argued that democracy is the best form of government because it has the best consequences. In a democracy, citizens are required to be involved, that is, to participate in the governance of the state. Thus, democracy calls upon the active capacities of its citizens. Moreover, individuals are the best representatives of their own interests. Democracy is, then, good for individuals and at the same time makes for a better state; citizens develop their capacities and the state benefits from the ideas that citizens contribute and from an informed citizenry.

In modern, large-scale, nation–states, democracy has meant that citizens have a right to elect representatives to the government, and these governments are accountable to the citizens. The size of nation–states has been a persistent and daunting challenge to the idea of democracy insofar as it has diluted the power of individual citizens to influence their government.

Throughout history, changes in technology have meant changes in the way democratic institutions have been constituted. Think here of how systems of communication have changed the content and speed of political decision making—not just in elections but in an array of domestic and international policy matters. For example, historically, new forms of transportation and communication have repeatedly changed the way democracies work.

A number of social commentators see the Internet as the latest technology to transform democratic practices and institutions. Perhaps the most obvious example of this is in the use of the Internet for political campaigning that now involves websites, blogs, e-mail, YouTube, and

more. However, the Internet has changed many other aspects of government in addition to campaigning. Consider, for example, how many government agencies have put public records online and made it possible for citizens to perform functions online; for example, submitting tax forms and paying traffic fines.

To get a handle on this very complicated set of issues, we can focus on the Internet and consider some of the arguments that are often hinted at, if not explicitly made, on behalf of a link between democracy and the Internet.

The Arguments

Many-to-many communication is probably the most prominent feature in these arguments. As described above, any individual who has access to the Internet can, in principle, communicate with any and every other individual who has access to the Internet. Before the Internet, this power was available only to a few, the few who had access to the broadcast capabilities of radio, television, or newspapers.

The arguments made on behalf of the democratic character of the Internet seem to link many-to-many communication to democracy in the following claims: The Internet: (1) allows individuals to be producers and distributors of information, (2) provides forums that are mediated differently than mass media, (3) facilitates access to many more sources of information, and (4) facilitates the formation of associations that are independent of geographic space. Let us consider each of these arguments in turn.

The Internet has empowered individuals to produce and distribute information by removing the traditional hurdles to doing so. Producing and distributing is easier and quicker when instrumented through the Internet. Of course, posting something on a website or distributing images through YouTube doesn't guarantee that anyone will pay attention; getting others to respond is another matter. Still, the system of information production and distribution is different and available to many more people. This is precisely the point of calling the Internet's scope many-to-many.

The Internet provides a variety of forums in which citizens can exercise their democratic right of free speech, and these forums bypass traditional media. Before websites, blogs, chat rooms, search engines, and YouTube, the primary means by which citizens could distribute information on a large scale was through mass media—newspaper and book publishers, radio, and television. As mentioned earlier, the hurdles to getting something distributed were huge—one had to buy advertising space in print and broadcast media, convince publishers to publish one's written work, or somehow get the attention of the press. The Internet has made the cost of information production and distribution so low that many can be providers as well as receivers.

It is tempting to say that the new forums differ from traditional media in being *un*mediated, but this would be misleading. Distributing and accessing information on the Internet is mediated, but it is mediated quite differently than traditional media. If in no other way, the architecture of particular systems mediates; distribution is skewed but in ways that differ from mass media. Distribution on the Internet reaches only those with Internet connections, those who understand the language in which the text is written, generally those who can see, and so on. Millions of people do not have access, and others have older equipment with reduced functionality. And this is not to mention the way the design of software packages, forums, interfaces, and service providers shape the quality and character of information. Thus, it is more accurate to say that distribution on the Internet is mediated differently than the distribution of information in mass media (rather than saying it is unmediated).

One of the consequences of lower barriers to production and distribution of information is that much more information is available. Citizens have access to more information and the information comes from a broader diversity of sources. The old saying that information is power is relevant here because those who distribute information have the power to shape those who receive the information—shape their attitudes, opinions, preferences, purchasing habits, and values. When the distribution of information is expensive and requires large institutional structures (as with radio and television), the few who control the media have concentrated power. With the Internet, that power is more decentralized and distributed

among the many who produce and distribute. Of course, the power of mass media has not, by any means, been eliminated. It has a presence on the Internet but its power is diluted by the broader range of other distributors.

That citizens can more readily be distributors and receivers of diverse information connects in important ways to John Stuart Mill's theory of democracy. He argued that democracy required that citizens exercise their active capacities and in so doing citizens and the state would continuously develop. Mill thought each individual's life would, in democracy, be an experiment in living that other citizens could learn from. In free societies, the best ideas emerge from the open combat of ideas. The Internet is a forum for just this sort of exchange. In effect, the Internet instruments interaction among citizens and draws on their capacities in particular ways and to a degree that was not possible before.

Yet another way in which these new forums for communication seem to contribute to democracy has to do with the formation of interest groups online. Whether the special interest is in a particular disease, a minority political position, a fetish, love of a particular kind of music, or a controversial idea, the Internet makes it possible for individuals to find others with the same interest. Of course, a wide variety of special interest organizations existed (and will continue to exist) offline. The difference the Internet makes is that associations can form and have frequent, immediate, and intense interaction *independent of geography*. When those who have a common interest are geographically dispersed, they are unable to identify one another, and hence, cannot act collectively; they have no means of working together, keeping each other informed, and making joint decisions. Separately, such individuals or groups are ineffective minorities. When they form associations online, they form communities and can act as such.

The possibilities for interest group formation online links directly to Madisonian democracy. James Madison argued that the best way for citizens to be heard in the political process was to form interest groups to put pressure on their representatives. The Internet has instrumented new means for forming such associations.

Is the Internet a Democratic Technology?

To summarize, the Internet might be considered a "democratic technology" because it: (1) allows individuals to be producers and distributors of information; (2) bypasses the traditional, concentrated power of mass media to distribute information (although is not unmediated); (3) provides access to a broader array of sources of information; and (4) facilitates the formation of interest group associations independent of geographic space. Do these claims justify the conclusion that the Internet **is** a democratic technology? They certainly identify patterns of behavior that are important for understanding IT-configured democracies. However, before drawing any conclusions, we should consider the arguments on the other side. Are there counterdemocracy patterns of behavior? Could the Internet be said to be a non- or undemocratic technology?

In discussing the argument about access to a wide variety of information resources, we noted in passing that although individuals can be the producers and distributors of information, this didn't guarantee that everyone would be heard or noticed. On the Internet, there is a good deal of competition for the attention of users. Moreover, because humans are limited in their capacity to absorb and effectively process and use information, we tend to need or find it helpful to have information filtered, selected, and routed to us. What sort of systems we have for filtering and sorting information becomes, then, an important matter. It is not at all clear that the current systems for this purpose are democratic. Are search engines democratic? What would a democratic search engine look like? Would it treat every bit of available information equal? How could it display information? Randomly? Would democratic search engines be useful?

Search engines are mechanisms for helping users identify the information they seek. To understand the democratic/nondemocratic character of the Internet, we would have to delve into the deep Web and understand exactly how various systems and algorithms order and route information. The algorithms make value decisions; they order information presented to users in a linear hierarchy. The lower down on the list, the less likely a user is to access information. Google keeps its algorithms secret. Although it has good reasons for doing so (so competitors cannot use them, and others cannot figure out how to "game" them), without access to the algorithms, we can only guess at the values that determine which websites appear

higher and lower in the list of relevant sites. On the other hand, we know that some sites are sponsored (paid for), because that information is displayed. Hence, we know that money (paying for a place) makes a difference. We would have to know much more about these algorithms to decide whether this component of the Internet is democratic. The very fact that we cannot examine these algorithms seems somewhat undemocratic.

Remember also that although the Internet facilitates many-to-many communication, it also facilitates one-to-many communication. The Internet is used by powerful institutions to maintain their power or dominance in an industry. The Internet is used as much to consolidate old associations and traditional hierarchies as it is to facilitate new forms of association. In short, although the Internet gives power to the less powerful, it also gives a new kind of power to the already powerful.

The controversy called "net neutrality" is an example of how powerful forces seek to control the Internet; in the net neutrality debate, some Internet Service Providers (ISPs) advocate that some content providers be allowed to pay for enhanced network speeds ("faster pipes"), but some large providers advocate to keep all Internet communications on equal footing ("dumb pipes" or a "neutral Net"). Although smaller content providers and individual Net users will be greatly affected by the outcome of this debate, it is the large ISPs and large providers that are contesting this issue. The chairman of the U.S. Federal Communications Commission (FCC) wrote, "This is essentially a battle between the extremely wealthy (Google, Amazon, and other high-tech giants, which oppose such a move) and the merely rich (the telephone and cable industries)." [Kennard, W. Spreading the broadband revolution. *New York Times* (Oct. 21, 2006), http://www.nytimes.com/2006/10/21/opinion/21kennard.html?_r=2&oref=slogin&oref=slogin, accessed June 5, 2008]. It was not lost on several commentators that policies of the U.S. FCC have been crucial in making the contenders extremely wealthy and merely rich. (For example, see [Lessig, L., 21st Century Reaganomics: Helping the "merely rich" so as to help the really poor (Oct. 23, 2006), http://lessig.org/blog/2006/10/21st_century_reaganomics_helpi.html, accessed June 5, 2008].) This is one example that

illustrates how the Internet is used to reinforce the power of governments and corporations in a way that is not accurately described as "democratic."

We should also not forget here that the surveillance capacity of the Internet (to be discussed in the next chapter) lends itself very well to totalitarian control. Remember, everything one does on the Internet endures. Traffic patterns, as well as content, are available to service providers (and hackers) and law enforcement agencies with a warrant. Private marketing agencies also want information about individual behavior on the Internet. This information is available through cookies. And, of course, the specter of China monitoring the e-mail and Web browsing activities of its citizens is probably alone enough for us to see that the Internet is not inherently democratic.

Another interesting, although perhaps ambiguous, challenge to the democratic character of the Internet is its global scope. In facilitating communication and interaction among individuals (regardless of their geographic location or nationality), the Internet has the potential to contribute to global democracy. However, this also could mean a weakening of nation–states. For good or ill, the many-to-many and differently mediated communication of the Internet makes it much more difficult for nation–states to control the flow of information to and from citizens and to control a wide variety of unlawful behavior. Although the Google in China case suggests a problem for totalitarian regimes, problems also arise for democratic regimes, for example, in enforcing legitimate laws that citizens are able to bypass.

Moreover, an intensely global economy (facilitated by the Internet) gives new economic opportunities to all involved, but at the same time pressures nation–states to harmonize their policies with other countries. This can be seen in a variety of areas where harmonization has been undertaken, including privacy and property rights policies. Whether or not harmonization is a good thing, that is, whether or not the policies are consistent with democratic values, depends very much on the particularities of the policy. Needless to say, the processes through which policies are harmonized are complex political and cultural negotiations. Although these negotiations can lead to improvements for democratic institutions and

practices, they can also go the other way. The Google in China case is, again, a good example here. (We will discuss these issues further in Chapter 6.)

Finally, it is important to remember that we have characterized the communication capacity of the Internet as many-to-many and not all-to-all. Even within a country like the United States, many individuals do not have access to the Internet, at least not convenient access. And, of course, globally the picture is even worse with billions of people without access. Thus, if democracy means that all those who are affected by a decision should be involved in the decision, the Internet has potential but we have a long way yet to go.

Is the Internet a democratic technology? This much seems clear: The Internet is not *inherently* democratic. Those who believe that it is probably think of the Internet as an artifact or technological system, but it is a sociotechnical system. It is much more than software, hardware, and telecommunications lines. Whether or not IT and the Internet facilitate democracy depends on all of the components of the system and that means the institutions as well as the artifacts. There are, as well, other reasons for eschewing such a broad and deterministic generalization as the claim that the Internet is inherently democratic. Those who believe this are likely to think that it is just a matter of time, and little needs to be done, before the adoption and use of the Internet will bring about global democracy. Nothing could be farther from the truth. The Internet is malleable and can support democratic and undemocratic patterns of behavior and institutional arrangements.

We conclude this discussion by mentioning the connection between democracy and freedom of expression, a topic that will be taken up more fully in Chapter 6, where we discuss what might be called "law and order on the Internet." Freedom of expression is generally considered not just essential to democracy but emblematic. Some would say a society isn't democratic unless its citizens have freedom of expression, at least a high degree of it. As we just described, the Internet enormously expands the possibilities for distribution of ideas and puts this capacity in the hands of many. Some describe the Internet as inherently free and even go as far as to

say that the Internet is not amenable to regulation, that is, that it is uncontrollable. We address this claim head on in Chapter 6.

Conclusion

The Internet and the World Wide Web have facilitated the formation of electronic communities, communities that transcend physical borders. As people increasingly interact via the Internet, our lives change because of choices made in configuring these online communities. Some of these choices are made by individuals, but many are made by governments, corporations, and technologists. Meanwhile, economic activities, educational activities, and social activities are all changing rapidly.

In trying to discern rights and wrongs in these new IT-enabled communities, we have used ethical analysis to examine three distinctive characteristics of IT communication: global, many-to-many scope; distinctive identity conditions; and reproducibility. We also explored the many complexities involved with the relationship between IT and democracy and IT and freedom of speech. In all these analyses, we emphasized that decisions, not "nature," drive the development of the Internet and of other IT systems. We contend that careful ethical analysis will make these decisions more visible, and will help societies make these decisions more wisely.

Study Questions

1. This chapter considers how technology should be conceptualized. What are the advantages of thinking about technology as the instrumentation of human action?
2. What is captured, and what is lost, when certain forms of IT are conceptualized as robots, and when human beings are conceptualized as cyborgs?
3. How does the scope of communication on the Internet differ from other forms of communication such as telephone, television, newspaper, and talking face-to-face?

4. Why is it not accurate to say that communication on the Internet is anonymous? What is different or distinctive about the identity conditions on the Internet when compared to identity face-to-face?
5. What is reproducibility, and why is it significant?
6. Did anyone do anything wrong in the virtual rape case? If so, who? What was the wrongdoing? Develop analogies between the behavior in this case and other kinds of behavior that occur offline.
7. Explain the statement that social networking sites shape, and are shaped by, friendship.
8. What characteristics of IT (and the Internet) change the environment for plagiarism and plagiarism detection?
9. Identify and explain the four arguments made to show that the Internet is a democratic technology.
10. Do any of the four arguments in question #9 hold up to critical scrutiny? Explain which argument you think holds up the best. Do you think that this best argument is convincing?

Chapter 4 Information Flow, Privacy, and Surveillance

Chapter Outline

Scenarios

4.1 E-mail Privacy and Advertising

4.2 Workplace Spying: The Lidl Case

4.3 Data Mining and e-Business

Introduction: Information Flow With and Without Information Technology

Why Care About Privacy?

"No Need to Worry"

The Importance of Privacy

Privacy as an Individual Good

Privacy as Contextual Integrity

Privacy as a Social Good Essential for Democracy

Autonomy, Democracy, and the Panoptic Gaze

Data Mining, Social Sorting, and Discrimination

Crude Categories

Summary of the Arguments for Privacy and Against Surveillance

Is Privacy Over? Strategies for Shaping Data Flow

Fair Information Practices

Transparency

Opt-In versus Opt-Out

Design and Computer Professionals

Personal Steps for All IT Users

A Note on Privacy and Globalization

Conclusion

Study Questions

Scenarios

Scenario 4.1 E-mail Privacy and Advertising

The following description of Gmail is taken from J. I. Miller, "Don't Be Evil": Gmail's Relevant Text Advertisements Violate Google's Own Motto and Your e-mail Privacy Rights" Summer, 2005, 33 *Hofstra Law Review* 1607:

> An attorney presses "send" on an e-mail message to a prospective client following an initial consultation. The prospective client has an e-mail account with Google's recently introduced Webmail service, Gmail. What the attorney does not know is that before his e-mail reaches its intended audience, Google will have scanned the contents of the message, found within it words and phrases such as "new client," "attorneys at law," "construction litigation," and even the name of the city in which the attorney practices, and placed along side the e-mail, contemporaneously with the client's viewing of it, advertisements for legal services offered by the attorney's competitors.

This seemingly hypothetical scenario is actually an everyday occurrence that is all too real.

Is there anything wrong here? If so, what?

Scenario 4.2 Workplace Spying: The Lidl Case

On March 26, 2008, Lidl, the second-largest grocery store in Germany, was accused by a German magazine (*Stern*) of hiring detectives to spy on its employees. The detectives installed cameras and microphones throughout the Lidl stores in Germany and the Czech Republic and they filled out reports on individual employees. Apparently, *Stern* obtained copies of these reports before making its accusations. According to one account, the detectives investigated workers, "both on the job, on cigarette and coffee breaks—and even on the toilet." The detectives gathered information on the financial status, relationships, and postwork activities of employees. On one account: "The transcripts also get into employees' private lives ('Her circle of friends consists mainly of junkies') and appearances ('Ms. M. has tattoos on both lower arms'). In their tone and detail, the observation logs invite comparison to those of the Stasi, the East German secret police." Particularly controversial is a report from the Czech Republic where, according to *Stern,* female employees were allegedly prohibited from going to the bathroom during work hours—unless they had their period, which they were to indicate outwardly by wearing a headband.

Lidl (which operates approximately 17,000 stores in 17 European countries) has not denied the accusations. Indeed, according to one account the company has apologized to its employees. The company attempted to justify the surveillance in terms of protecting their stores from employee theft.

The accusations are apparently being investigated by a government ombudsman for data protection. Lidl's surveillance practices may constitute violations of personal privacy and human dignity as specified in German statutes and, perhaps, their constitution.

Based On

Anonymous. 2008. "Two More German Chains Caught Spying on Employees." in *Der Spiegel Online*, April 3. <http://www.spiegel.de/international/germany/0,1518,545114,00.html> (Accessed May 9, 2008).

—. 2008. "Discount Chain Accused of Spying on Others." in *Der Spiegel Online*, March 26. <http://www.spiegel.de/international/business/0,1518,druck-543485,00.html> (Accessed May 9, 2008).

Walderman, A. 2008. "Lidl Accused of Spying on Workers." in *Businessweek*, March 26. <http://www.businessweek.com/print/globalbiz/content/mar2008/gb20080326_558865.htm> (Accessed May 9, 2008).

Scenario 4.3 Data Mining and e-Business

The following description of consumer profiling in e-business is taken from Oscar H. Gandy, Jr., "All that glitters is not gold," *Journal of Business Ethics* 40 (2002): 373–386:

> Carol is interested in purchasing a new computer and she visits TechStation.com, an electronics e-tailer. Carol is a first-time visitor to this site. After entering a few keywords to search the site and after browsing through several of the pages she selects the model she is interested in. Carol adds a printer to her virtual shopping cart and continues browsing. The observational personalization system used by the electronics store compares her point of entry to the site, the keywords she used in her initial search, her clickstream within the corporate site, and the contents of her shopping cart to the navigational patterns of existing customers already in [the] firm's database. Through this comparison, the system fits Carol into the "young mother" profile that it developed by mining the Web navigation logs generated by previous visitors and existing customers. Accordingly,

the recommendation engine offers Carol a discounted educational software package before she checks out.

Carol was, in fact, not a young mother, but a middle-aged divorcée. She purchased the computer and printer she was interested in, but did not find the time management software she actually wanted to buy. A bit frustrated, Carol leaves the site in search of the software she needs. At about the same time, Steve entered the site and selected the same computer and printer. Although he chose the same products as Carol, Steve did not receive the same offer for discounted educational software. He entered the site from a different portal than that used by Carol; he had a different clickstream pattern from hers, and he used different terms in his keyword search. Steve's navigational pattern resulted in his being assigned to a different profile. Steve fit best into the "college student" profile and, as a result, he was offered a discount on a statistical software package. In fact, Steve is an English major. Like Carol, Steve's projected needs did not accurately match his real needs.

Is TechStation.com doing anything wrong? What, if any, information would help you decide whether the company is doing anything wrong? What ethical issues does this situation raise?

Introduction: Information Flow With and Without Information Technology

In an IT-configured society, information flows quickly and easily and in a variety of directions. In hindsight, it seems that before IT the flow of information was "constrained" by the technologies in use at the time—mechanical typewriters produced one copy (or at most a few more with the use of carbon paper); cash registers recorded the amount of a purchase but didn't create records of who bought what; mail delivery systems were slow, cumbersome, and variable. IT changed all of that and facilitated unprecedented flows of information.

All three of the characteristics we identified in the last chapter come into play in privacy and surveillance issues. Perhaps the most prominent feature is reproducibility because if it weren't for reproducibility, information would still be difficult to distribute and manipulate. Although we emphasized in Chapter 3 that information flows globally from many-to-many, we also noted that it flows in all directions including one-to-many, one-to-one, and many-to-one. Privacy and surveillance issues are primarily concerned about *personal* information, that is, information that is about a particular person. In this respect, the identity conditions of the Internet also come into play in privacy and surveillance issues because it is difficult (and often practically impossible for most) to operate online without being tracked in several ways.

To comprehend the significance of privacy and surveillance issues, it will be helpful to compare information flow today with that before the development and widespread use of IT for personal data collection. Notice first that the *scale* of personal information gathering has expanded exponentially. In the "paper-and-ink" world, not only was it costly and labor intensive to collect information, but it might not even have been considered because the paper and ink world didn't make it ready at hand. The fact that records were paper and stored in file cabinets imposed limitations on the amount of data gathered as well as who had access and how long records were retained. Electronic records have none of these limitations; they are easy to create, store, maintain, manipulate, search, and share. Thus, many more records are created and used.

Of course, we should be careful here not to slip into technological determinism. IT didn't cause organizations to gather and process so much information. Companies have always had interests in identifying and understanding customers and clients. As well, they have always had interests in getting information about their products to potential customers. Similarly, governments have always had interests in knowing about citizens. To be sure, these interests have been shaped by the development of IT; but IT was shaped in response to the interests of corporations and governments. Database management systems, datamining tools, and cookies weren't invented out of nowhere. Software and hardware developers developed tools that business and government would want to

buy and use. Thus, information gathering and manipulation practices shaped, and were shaped by, IT.

In addition to an increased scale of information gathering, IT has made for new *kinds* of information. Transaction generated information (TGI) didn't, and in some sense couldn't, exist before IT. TGI is automatic and seamless. In the past when I bought something, I gave the clerk cash or wrote a check; now I provide my credit card, the card is swiped, and a record is created. The record resides in a server (or servers) somewhere in the world; that record can be accessed from any number of places, downloaded, and forwarded.

Of course, today I may not even go into a store; I simply go online and provide my credit card information. Other important forms of TGI involve the use of cookies that record the websites people access and "clickstream," as described in Scenario 4.3. When personal information from various places is merged and mined, this also produces new kinds of information. For example, although profiles of individuals were produced before IT, profiles today are expanded and much more detailed. When matched against databases of information about others, they have much more predictive power than those of the past.

Today, distribution of personal information is broader and more extensive than it was ten or twenty years ago. Before computers were connected to telephone lines, information could not move as easily as it now does. A transaction record or change in one's credit rating can instantaneously move to anywhere in the world where there are electricity and telecommunications connections. Once information about an individual is recorded on a server, it can be bought and sold, given away, traded, or stolen. The distribution of information can take place with or without the knowledge of the person whom the information is about, and it can take place intentionally as well as unintentionally.

In addition to the scale of information gathering, kinds of information, and scale of information distribution, information tends to endure for much longer periods of time. When information is stored electronically, there may be little incentive to get rid of it. In the past, the inconvenience of paper and the cost of storage served to some degree as an inhibitor to keeping and

exchanging information. This endurance is illustrated through the recent controversy over personal information and images on Facebook. Facebook maintains records of all sites and it has recently come to public attention that users—even when they cease to be users—may not be able to delete information from Facebook. There is some indication that images in particular continue to be available even after one closes one's Facebook account. [See: http://news.bbc.co.uk/2/hi/technology/7196803.stm and http://epic.org/privacy/facebook/default.html]

Note here also that we have said nothing about the quality or accuracy of the information that flows. Errors in information arise due to unintentional human error or may have occurred intentionally, for example when someone tampers with data because they want to harm a competitor or enhance their own position. When there is an error in personal information, the effect of the error can be significantly magnified; the erroneous information may spread so quickly that it is impossible for an individual to track down all the places it exists. Of course, those who want information about individuals want accurate information, but when faced with a choice between little or no verifiable data and data that may or may not be unreliable, decision makers may prefer the latter.

So, in IT-configured societies: (1) much more personal information is collected, (2) new kinds of personal information are created, (3) personal information is distributed more widely, (4) this information endures for longer periods of time, and (5) the effects of erroneous personal information are magnified. How does privacy fit into this relatively new kind of society?

Why Care About Privacy?

All of this means that individuals in IT-configured societies are intensively tracked and monitored. Surveillance may occur: through closed circuit television cameras (CCTV) when we walk on public streets or attend events in public spaces, on the computers we use at work as supervisors monitor our work, as the navigational devices installed in our automobiles identify our location to give us directions to our destination, through our cell phones as service providers locate our phones to direct calls to us, and when websites track our browsing and searching so that they can customize

assistance with our searches and shopping. The data collected in each one of these contexts can then be merged to create comprehensive profiles of individuals. Combinations of data can also be "mined" to find patterns and correlations that might not otherwise be obvious. Individuals in this age range or that income level tend to buy these sorts of items or are more likely to be terrorists or to default on loans. It is not surprising, then, that IT-configured societies are often characterized as "surveillance societies."

Our task in this chapter is not just to describe how personal information flows but to examine the significance of this flow critically and normatively. To this end we must ask questions of the following kind: What, if anything, is the value of privacy? If privacy disappears, what exactly will be lost? How does surveillance affect social arrangements, institutions, and practices? What sort of beings do we become when we live in surveillance societies?

We will begin to answer these questions by making the best utilitarian case we can *for* surveillance, that is, for the kind of personal information gathering and distribution processes that are common in information societies. As we move to the case *against* surveillance and *for* privacy, the frame of the argument will start with a utilitarian analysis and then shift away from utilitarianism toward arguments based on autonomy and democracy.

"No Need to Worry"

Those who think we need not worry about intensive tracking and monitoring of individual behavior can, it would seem, make the following arguments. First, they can argue that if you aren't doing anything wrong, you should have no need to worry about being watched. Second, they can argue that privacy is overrated; they can point out that those who live in IT-configured societies have, in fact, let privacy go and this is evidence that privacy is neither valued nor valuable. Finally, they can argue that the information that organizations gather about individuals has enormous benefits to the organizations that gather it as well as to the individuals the information is about. We will consider each of these arguments in turn with a critical eye.

According to the first argument, if you haven't broken the law—if you are doing a good job at work, paying your bills on time, not doing anything illegal online or off—then you have no need to worry; nothing bad will happen to you from being watched. Someone putting forth this argument might go as far as to say that "privacy only protects people who have something to hide."

Unfortunately, the effects of personal information flow are much more complicated and not always as benign as this argument suggests. Remember that erroneous information can dramatically affect your life even if you have done nothing wrong. Suppose you are traveling away from your home and the police begin chasing your car. They point guns and rifles at you and force you to get out of your car. They frisk you. If you panic and respond suspiciously, you could be beaten or killed. Suppose further that the police officers believe you are driving a stolen vehicle and they disregard your explanation that the car is yours. You try to explain that it had been stolen, but was found last week and returned to you by the police in the city where you live. You find out later that when you reported the car stolen, the information was put into a database available to patrol cars in several bordering states. Evidently, however, the information that the car had been found and returned to its owner never made its way into the database for the patrol cars in this state. Aside from the increased risk to which you have been exposed, we might further suppose that it takes the police officers a day to confirm the truth of your claim that you were driving your own car. So, even though you have done nothing wrong, you may spend a night or two in jail and miss out on whatever you had been planning to do. That night in jail is almost certainly recorded electronically and the record of your incarceration can itself become an issue. For example, years from now you may lose an opportunity for a new job because a prospective employer finds a record of your jail time in a database, and doesn't even interview you despite your otherwise spotless record. You have been harmed even though you did nothing wrong. You also may not even be aware of the record of that night in jail, and you may never know why your life is being changed because of it.

Lest you think that erroneous information is rare, consider that in May of 2008, the Electronic Privacy Information Center (EPIC) filed a "friend of

the court brief" in the U.S. Supreme Court urging that the accuracy of police databases be ensured. Describing how unreliable government databases have become, the brief urges the Court to "ensure an accuracy obligation on law enforcement agents who rely on criminal justice information systems."

In any case, the problem is not just that erroneous information can lead to decisions that are harmful to individuals. There is also the issue of irrelevant information—information that would be inappropriate or unfair for an organization to use. Remember in Scenario 1.2 in Chapter 1 how information posted on a social networking site (so that friends might see it) is used by a company to make a hiring decision. U.S. Title VII of the Civil Rights Act of 1964 prohibits employers from discriminating against applicants and employees on the basis of race or color, religion, sex, and national origin, yet when this information is readily accessible, it can be used without impunity. To make the point salient, consider a case reported some time ago. Forester and Morrison (1990) tell the story of a woman who took her landlord to court after he refused to do anything about the pest problem in her apartment. He did not show up for court but evicted her shortly after the court date. When she went looking for another apartment, she found that she was repeatedly turned down by landlords. She would look at an apartment, fill out an application form, and within a short time be told that the apartment was already rented to someone else. She later discovered that a database of names of individuals who take landlords to court was maintained and sold to landlords. Needless to say, landlords don't want to rent to individuals who are likely to take them to court. So here we have a case in which an individual experiences severe negative consequences for exercising her legal right to take her landlord to court.

Thus, it isn't true to say that if you do nothing wrong, you have no need to worry. Use of erroneous information may result in you being denied a benefit you are entitled to—a loan, a job, an educational opportunity—or subjected to treatment you don't deserve—being held up at an airport, arrested, being harassed by a collections agency. And, even when information is accurate, it can be used inappropriately to make decisions for which the information is irrelevant or even illegal to use (for example, when your race, religious affiliation, or sexual preference is used inappropriately).

The second no-need-to-worry argument is that privacy is overrated—people have traded it off for benefits, so it must not be valued or valuable. In support of this argument, consider that many of us give up privacy with regard to our purchasing habits when we shop online or at grocery stores where we use membership cards in order to receive discounts. Of course, companies make an effort to inform customers about their privacy policies, but consumers seem largely unaware of these policies and readily trade their personal information in exchange for discounts.

Although it may be true that individuals trade off privacy for what may seem like small benefits, it is unclear how this behavior should be interpreted. The fact that individuals readily give out personal information doesn't mean, necessarily, that they don't value privacy, or that privacy isn't valuable. They may be naïve and uninformed about the choices they are making, and/or they may just be wrong. The consequences of giving up personal information may be so distant from the act of disclosing it that individuals do not accurately perceive the negative consequences. The choices available to individuals when they opt to give out personal information may be constructed in such a way that individuals may be unknowingly choosing against their own interests. For example, often we are given only the choice to take the benefit (say a discount) in exchange for disclosure of information *or* not get the benefit at all. If individuals had more options, they might well choose more privacy. The bottom line here is that it is difficult to interpret the meaning of the choices that individuals are making about their personal information.

Another problem with the privacy-is-overrated claim is that even when individuals reasonably choose to give up privacy in a particular context, they are never given a choice with regard to the overall character of their society. What seems to be a choice about a *local* sharing of information may actually be a choice for *global* sharing, and so people are making a series of seemingly small choices without realizing the large cumulative effects of those choices. The cumulative effects of giving up privacy in this or that sector may not be evident when we focus on privacy in each particular domain separately. When considered separately, giving up privacy in online shopping may look benign, giving up privacy in air travel may seem reasonable, and submitting to closed circuit television monitoring

in public places may not seem problematic. However, when it is all added up, we may find ourselves with little privacy at all.

In summary, there doesn't seem to be conclusive empirical evidence to support the claim that individuals don't value privacy.

The third argument is that personal information-gathering practices can be beneficial to information-gathering organizations and to their customers and subjects. This is a strong argument. Information-gathering organizations wouldn't be gathering personal information if they didn't think it would help them, and it often helps them in ways that improve their products and services. Thus, customers and clients can both benefit. Information about individuals helps organizations to make decisions and, arguably, the more information they have, the better the decisions. For example, the more information mortgage lenders and banks have about an individual, the better they should be able to determine the applicant's ability to pay back a loan. The fewer loan defaults there are, the more efficient the service, the lower the cost to borrowers. The more information that law enforcement agencies have about individuals, the better they are able to identify and capture criminals and terrorists—something from which many of us benefit. If television stations know what we watch on television and when we change the channel, they can use that information to develop programming more suited to our tastes. If marketing companies know our income level, and tastes in clothes, food, sports, and music, they can send us customized information and special offers for precisely the products that are affordable and fit our tastes.

On the other hand, there is some question as to whether organizations use the information they collect and manipulate to *serve* their customers, clients, and citizens. Indeed, there is considerable evidence that organizations use the information to *shape* their customers. There is also some question as to whether these organizations use appropriate information when they make decisions about individuals. Whether or not their decisions are justified or fair depends both on whether the information used is accurate and whether the information is relevant to the decision. Here the matter gets complicated, because information-gathering institutions use information about us in ways that have powerful effects on

our lives, and appropriate use is essential to whether we are being treated fairly.

Although we have countered the first two of the no-need-to-worry arguments, the third requires more extended analysis. The third argument is utilitarian; the claim is that the intensive and extensive gathering and flow of personal information has significantly good consequences. Remember now that in a utilitarian framework, we must consider not just the positive consequences of a practice; we must consider both the positive and negative, and not just the consequences for some of those who are affected but for all of those who are affected.

The Importance of Privacy

Why, then, should we worry? What happens when personal information flows intensively and extensively in IT-configured societies? What is at stake here? Concern about the loss of personal privacy was the first public issue to gain significant attention when computers were first developed and databases of personal information began to be used by government agencies and private corporations. Privacy continues to receive a good deal of public attention, although over the years much of the battleground of privacy has shifted to a set of debates about personal information in different domains —credit records, workplace surveillance, airport screening, medical records, and so on. There has also been a conceptual shift to focusing on surveillance—information-gathering practices—as a supplement to the focus on privacy.

Privacy as an Individual Good

When the threat to privacy from IT-based practices first came to public attention in the 1970s, the issue was framed as a public policy issue, an issue calling for a balance between the needs of those who wanted information about individuals *and* the interests, preferences, or rights of the individuals who the information was about. It is important to note that in this framework it is primarily organizations—national, state, and local government agencies and private organizations—that are interested in

information about individuals, and these organizational interests were seen to be in tension with individual interests or rights.

Early concerns about privacy focused on whether individuals could be said to have a legal, constitutional, or moral "right" to privacy. Of course, the arguments for a legal as compared to a constitutional or moral right are very different. In addition, privacy in relation to government differs from privacy in relation to the private sector. In the United States, legal notions of privacy can be traced back to two of the Amendments to the Constitution. The first amendment addresses freedom of speech and the press; the fourth amendment proscribes unreasonable search and seizure, and insures security in person, houses, papers, and effects. These two amendments deal, respectively, with the relationship between the government and the press, and between the government and the individual. The American forefathers were concerned about protecting citizens from the power of government. They did not envision the enormous power that private organizations have come to have over the lives of individuals. Corporations are often treated in law as persons in need of protection from government, rather than as powerful actors that need to be constrained in their dealings with individuals. Thus, the challenges of establishing rights of privacy in relation to private corporations are especially daunting.

The arguments for a "right" to privacy have been enormously convoluted and not nearly as successful as many had hoped (with the idea that a privacy right might "trump" other interests). Establishing that citizens have a "right" to something that is not explicitly stated in a historical document, such as the American Bill of Rights, is complicated in the sense that the right must be inferred from other rights, case law, common law, or other precedents. Legal rights can be created by means of legislation and, therefore, it is true that citizens of particular countries have certain kinds of privacy rights. For example, American citizens can refer to the Privacy Act of 1974 to understand their rights, and citizens of countries that are members of the European Union (E.U.) can refer to the E.U. data protection laws.

Our strategy here is not to focus on rights—legal or otherwise—but rather to try to understand broader concerns with regard to the importance of

privacy. We will not argue that all data gathering and surveillance is bad, nor will we argue that privacy should always trump other values. Rather, we will argue that privacy is a complex value that is intertwined with autonomy, equality, and democracy, and its importance ought to be recognized in IT-based practices.

To begin to make the case for the value of privacy, we can return to the distinction made in Chapter 2 between instrumental and intrinsic values. Is privacy an instrumental value or an intrinsic value? That is, is privacy good because of what it leads to (enables) *or* is it good in itself? The standard arguments that have been made on behalf of privacy as an instrumental good take privacy to be instrumental for certain kinds of human relationships or for a diversity of such relationships. Fried (1968), for example, argued that friendship, intimacy, and trust could not develop in societies or contexts in which individuals were under constant surveillance. This argument was consistent with ideas hinted at in early twentieth-century science fiction works concerned with totalitarian control, works such as George Orwell's *1984* (1949) and Zamyatin's *We* (1920). These authors envisioned worlds in which individuals were continuously watched, and they suggested that in such societies it would be difficult, if not impossible, to have truly intimate moments, moments in which an individual might reveal his or her vulnerabilities, and establish intimacy with others. When individuals are being watched, it is impossible, they suggested, to develop trust and mutual respect.

Although a threat to friendship and intimacy does not seem to be at the heart of concerns about personal privacy today, the idea that privacy plays a role in *relationships* does seem to point in the right direction. Rachels (1975) put forward another, related argument that seems to get closer to the heart of the matter. Rachels argued that privacy is necessary to maintain a *diversity of relationships*. He was thinking about privacy as the control of information about yourself, and his important insight was that the kind of relationships we have with others—our parents, spouses, employers, friends, organizations—is a function of the information we have about each other. If everyone had the same information about you, you would not have a diversity of relationships. Think, for example, about what your best friend knows about you as compared with what your teacher, your employer, or

Google knows about you. Or think of the differences between friends that you know only online and those that you interact with on- and offline. If we cannot control who has what information about us, it would seem that we couldn't have the diversity of relationships we have.

Taking this a step further, suppose that you have been seeing your current dentist for the last five years and she knows relatively little about you, except, of course, when it comes to your teeth. Now suppose you need extensive work done on your teeth, and you begin to go to her office regularly at a time of the day when she is not rushed. You strike up conversations about your various interests. Each time you talk to her, she learns more about you, and you learn more about her. Suppose you discover you have several hobbies and sports interests in common. You check her out on Facebook. You begin to chat online. At some point, she suggests that if you schedule your appointment as her last appointment of the day, you could go out and have a drink together afterwards. The relationship develops from one of patient–professional, to friends, perhaps to good friends, and it might eventually develop into an intimate or lifelong relationship. Notice that the changes in the nature of the relationship are, in large measure, a function of the amount and kind of information you exchange about one another.

Rachels's argument is, then, that we need privacy (control of information about ourselves) because it allows us to have a diversity of relationships; privacy is "instrumental to" a diversity of relationships. Of course, Rachels seems to presume that a diversity of relationships is intrinsically good, or he may be presuming, like Fried, that a diversity of relationships is good because it allows for friendship, intimacy, and trust which are intrinsically good. The important point in Rachels's argument is not, however, the focus on a diversity of relationships, but rather the idea that relationships are a function of information. Rachels understands that we control the nature of the relationships we have by controlling the kind of information we reveal about ourselves.

Unless we are careful here, Rachels's account may point us in the wrong direction. It would seem that the intense and wide ranging flow of personal information in information societies tends to facilitate a diversity of

relationships. Social networking sites, chat rooms, and blogs open up more avenues for relationships and therefore more diversity of relationships. Similarly, when a company acquires information about you, infers that you would like their products, and sends you advertisements and special offers, you have acquired an additional relationship. The same could be said about a law enforcement agency that finds you in a database search of individuals who belong to Muslim organizations. However, in the latter cases, although you have a wider diversity of relationships, you haven't had much say in the creation of these relationships. Adding unwanted relationships may increase the diversity of your relationships, but this kind of diversity doesn't seem valuable. The value of a diversity of relationships is more complicated than Rachels suggests.

To get to the heart of the matter, we need to take Rachels's argument a step further. Gossip provides a good illustration of Rachels' idea that when we lose control of information, we lose control of relationships. When gossip about you is being circulated, you may feel threatened by the loss of control you have over your personal information. When others are gossiping about you, you don't have any control over what is being said about you and to whom the information is being given. You cannot control what people will think about you and you cannot control how they will treat you. Individuals have an interest in being viewed and treated in certain ways, and information affects how one is viewed and treated. Once the information begins to move from person to person (and organization to organization), you have no way of knowing who has what information about you. If the information is false, you have no way of contacting everyone and correcting what they've been told. Even if the information is true, there may be individuals who will treat you unfairly on the basis of this information. Yet because you don't know who has the information and whether or how it is being used, your ability to control how you are being treated is diminished.

The gossip example suggests that control of personal information is a means by which we control the relationships we have and how we are treated in those relationships. In short, control of information about ourselves is an important component of our autonomy. If we have little say in how we are treated, we are powerless. Of course, this doesn't mean that individuals should have absolute control of all information about

themselves but it points to a connection between privacy (as control of information about one's self) and autonomy. This insight can be developed in two different directions. The first emphasizes contextual norms and the second emphasizes democracy.

Although the gossip example explains why we might want to control personal information, we cannot expect others to make decisions about us without information. Information about us flows in everyday life when others see us, hear what we say, and interact with us. This information flows from one person to another and individuals have little control of how others interpret the information. Moreover, we cannot expect to hide certain kinds of information when we are in particular contexts or relationships. For example, if you apply for a loan, it is reasonable for the lender to ask about your financial condition—for example, your income, assets, and debts. If you apply for a job, it is appropriate for the employer to ask about your employment history, education, and experience. Ideally, perhaps we should be able to control information and release it only when we choose to enter a particular context, that is, when we request a loan, purchase a ticket for an international flight, or have a medical bill covered by an insurance company.

When it comes to privacy, our attention should be on information practices in particular domains rather than on privacy in some broad or amorphous sense. The simple question about the value of privacy turns into a set of questions about what kind of information should flow, where it should flow in particular contexts, and who is allowed to control it.

Privacy as Contextual Integrity

Nissenbaum's account (2004) of privacy as contextual integrity does exactly what is called for. The account begins with the insight that there are information *norms* in every domain of life. The norms vary from domain to domain but in each context individuals have expectations about: (1) what kinds of information are appropriate and inappropriate, and (2) how that information will be distributed. According to Nissenbaum, then, when information norms are violated, an individual's privacy is violated. When you apply for a loan at a bank, you reasonably expect that the bank will

inquire about your salary, financial assets, and debts, but you would be surprised and dismayed if the bank asked about your ethnic background, political affiliations, medical history, or sexual preferences. On the other hand, in the context of receiving health care, you would expect to be asked about your medical history; you might even expect that some of the questions about your medical history might connect to your ethnic background or possibly even your sexual preferences (although you wouldn't expect this to happen if you went in to have a broken arm set). You would not expect, in the medical context, to be asked about the details of your financial investments or political affiliations. All of this shows that there are norms with regard to what is appropriate information in particular contexts.

Similarly, there are norms about how the information revealed in particular contexts will be distributed. In the United States, cash purchases of $10,000 or more must be reported to the Internal Revenue Service. When it comes to criminal records, there are restrictions on who can access particular kinds of records as well as requirements for disclosing records to other agencies. Distribution of medical records is also restricted. On the other hand, credit reports are widely distributed to those who request them and are willing to pay. Norms for friendship are such that when you share embarrassing information with your best friend, you don't expect to see what you said posted on your friend's blog. If you do, you may reevaluate that friendship.

Information norms—norms with regard to appropriate/inappropriate kinds of information and distribution of information—are both formal and informal. Formal norms are established and explicitly stated in legislation or specified in organizational policies that are made available to employees or customers or the public. Individuals can sue organizations that violate formal norms. Other norms are informal and conventional; they are enforced primarily by social expectations and social pressure. In the United States, for example, it is generally considered impolite to ask someone—even someone you know fairly well—how much money they make. Although you might tell your close friends about your love life, you would be surprised if someone you met for the first time were to ask you about your latest romantic entanglement. Many of these informal information norms are subtle, and often they are unclear. They can vary widely in

different cultures and countries. For example, although doctors and lawyers are formally expected to keep information about their patients/clients confidential, conventions with regard to what you tell your hairdresser, car mechanic, or coach are unclear. In a small town in Italy the norms about sharing personal information may be dramatically different from the norms in Tokyo.

Norms also can change over time as institutions and practices change. To change a formal norm, a new law may be enacted or a new public statement of policy issued. Change in informal information norms is common, especially as part of broader social and cultural change. Importantly, changes in information norms are often triggered by a change in technology. Remember that IT expands the possibilities for information creation and flow. This has constituted situations that fit Moor's notion of a policy vacuum. Organizations may—with adoption of a new technology—be able to create and distribute new forms of information and there may be no preexisting norms with regard to whether or how the new type of information should be used or distributed. Often norms evolve in a rather ad hoc manner with organizations simply using whatever technology is available to them while their clients, consumers, and the public are unaware of the practices until some event occurs, such as the government demanding records of weblogs. Only then do users become aware of the data that their ISPs collect. Scenario 4.1 is a good example here. Users have only recently discovered that Google can and does search e-mail for content.

Nissenbaum's account of privacy as contextual integrity draws our attention to information norms and how they vary with context. Her account implicitly explains why privacy policy debates have centered on legislation and policies for particular domains; information norms have to be worked out for particular sectors or contexts. The account also helps us to understand why privacy is so difficult to protect. IT tools are often invisible in the domains in which they are used and they are adopted and used without public announcement. Thus, customers, clients, and citizens are unaware of information norms in many contexts. They have no reason to inquire, and no way of finding out, whether information norms are being adhered to. Without knowing the norms and whether they are being adhered to, one doesn't know whether one is being treated appropriately or not.

Were we to follow this stream of analysis further, we could delve more deeply into domains in which information is particularly sensitive or especially powerful. For example, medical information is particularly sensitive, and employee monitoring is powerful in part because individuals spend so many hours of their lives in the workplace. However, we turn now to another stream of analysis that follows from our focus on control of information about ourselves and the connection between privacy and autonomy.

Privacy as a Social Good Essential for Democracy

We arrived at this point in our analysis by thinking about privacy as an individual good and asking about its importance to individuals in their relationships with others, be it with organizations or other individuals. This strategy has recently been called into question by those who point out that, in many cases, arguing for an individual interest in (or even right to) privacy has not succeeded in convincing policy makers to give individuals control over personal information. When privacy is treated as an individual interest and then pitted against the interests of public and private organizations in a utilitarian cost-benefit framework, organizational goals and interests have trumped the interests of individuals. The U.S. Patriot Act is a good case in point. In the face of the threat of terrorism, and in the interest of security, this legislation gave enormous power to security agencies to gather information about individuals without much protection for their privacy or civil liberties.

In her 1995 book, *Legislating Privacy*, Priscilla M. Regan examined three privacy policy debates that took place in the United States—information privacy, communications privacy, and psychological privacy. She concluded that when individual privacy is balanced against social goods such as security and government efficiency, personal privacy loses. Regan suggests that instead of framing privacy as an individual good, we should understand it as a social good. As a social good, privacy would be on par with other social goods such as security or efficiency. Although privacy might not always trump the other social values, it is much more likely to get a fair hearing when it is understood as a social good. Think here of the utilitarian calculus; when social good is balanced against the good of some

individuals, social good generally wins. However, when two social goods are pitted against each other, both must be taken into account.

How, then, can we make the case for privacy as a social good? We can do this by returning to our discussion of a connection between privacy and autonomy but think of autonomy not just as an individual good but rather as essential to democracy. To understand this connection, we can consider an observation that a number of privacy theorists have made about information societies. They have observed that living in an IT-configured society is similar to living in a "panopticon"—a structure designed by Jeremy Bentham (1787) to serve as a prison.

Autonomy, Democracy, and the Panoptic Gaze

Bentham's prison was designed so that the chambers in which prisoners lived would be arranged in a circle and the side of each cell facing the inside of the circle would be made of glass. The guard tower would be placed in the middle of the circle, so a guard standing in the guard tower would have full view of every chamber. The prison design did not allow for two-way observation; that is, the prisoners could not see the guard in the tower. The idea of the panopticon was picked up by Michel Foucault in 1975 and brought to wider public attention. The claim that is often made about both writers is that they both understood the power of surveillance (continuous observation). They understood that surveillance affects the behavior of those who are observed. In the panopticon, a prison guard need not even be there at every moment; as long as prisoners believe they are being watched, or at least believe that they are probably being watched, they will adjust their behavior and adhere to the norms they believe the guards want to enforce.

Although interpretations of this effect vary, part of the effect of the "panoptic gaze" is achieved by individuals internalizing the views of their watchers. When individuals believe they are being watched, they are compelled to think of themselves as their observers might think of them. Thus, they come to see themselves as their watchers see them, and this leads the individuals both to experience themselves in relation to the

watchers' norms and to behave quite differently than they might if they were not aware of being observed.

In IT-configured societies, if much of what we do is recorded and likely to have future consequences in the way we are treated, then we have to consider our watchers and their norms whenever we act. On the one hand, this effect may have positive consequences; for example, we are more likely to abide by the law, be careful about our debts, stay focused at work, and so on. On the other hand, our freedom and autonomy are diminished, especially when we have had little say in setting the norms. It is not just that we have to be careful about abiding by the law or paying our debts; we also have to be careful about what we post on our Facebook sites, what we search for on Google, what law enforcement officials might make of our phone calls to the Middle East, and who knows our sexual preference, drinking habits, religion, and so on. There are at least two quite different concerns here. The first is the dampening effect on our freedom (autonomy). The second can be seen by asking who are our watchers, and how have they selected the norms of behavior by which they evaluate us?

The dampening effect on freedom is significant but it is not just a matter of narrowing our freedom. Surveillance undermines our ability and capacity for democratic citizenship. Living in a panopticon means that individuals have very little space to develop themselves independently; they have little opportunity to develop autonomy. Jeffrey Reiman (1995) puts the point sharply:

> To the extent that a person experiences himself as subject to public observation, he naturally experiences himself as subject to public review. As a consequence, he will tend to act in ways that are publicly acceptable. People who are shaped to act in ways that are publicly acceptable will tend to act in safe ways, to hold and express and manifest the most widely-accepted views, indeed, the lowest-common denominator of conventionality. . . . Trained by society to act conventionally at all times, people will come so to think and so to feel. . . . As the inner life that is subject to social convention grows, the still deeper inner life that is separate from social convention contracts and, given little opportunity to develop, remains primitive. . . . You lose

> both the practice of making your own sense out of your deepest and most puzzling longings, and the potential for self-discovery and creativity that lurk within a rich inner life. . . . To say that people who suffer this loss will be easy to oppress doesn't say enough. They won't have to be oppressed, since there won't be anything in them that is tempted to drift from the beaten path.

The idea of democracy is the idea that citizens have the freedom to exercise their autonomy and in so doing develop their capacities to do things that have not been thought of before. Democracy requires citizens who are capable of critical thinking, individuals who can argue about the issues of the day and learn from the argument so that they can vote intelligently. All of this makes for a citizenry that is active and pushing the world forward progressively. But if the consequences of trying something new—an unconventional idea, a challenge to authority—are too negative, few citizens will develop the capacity to take risks. Democracy will be lost.

The argument for privacy is, then, an argument for the space that individuals need to develop autonomy. When the argument for privacy is framed in this way, privacy is shown to be something that is not just an individual good that can be diminished for the sake of a social good; rather, it is shown to be a social good, such an important social good that it should not be eliminated when it comes into tension with other social goods, even if the social good is security and certainly not if it is better consumer services.

The connections between privacy, autonomy, and democracy are so close that it doesn't seem accurate to say that one is instrumental to the other. Privacy, autonomy, and democracy are so intertwined that one is inconceivable without the other. Privacy is not just "instrumental to" autonomy or democracy; it is essential to both.

Data Mining, Social Sorting, and Discrimination

We can take this argument further by noting that the problem is not just that we are being tracked and monitored; the norms by which we are being

measured, evaluated, and treated are often not subject to public discussion and negotiation. Often they are invisible to the individuals being watched, evaluated, and treated. When it comes to governments and government agencies, the norms may well have been established through a political process, for example, the Patriot Act, although even then in many cases the norms are kept inaccessible in the name of security. In other cases as with online tracking and marketing, there may be no rationale given or information may be protected by trade secrecy laws. In either case, those who are watched may not know they are being watched, or may know they are being watched but not know how the information is being collected or used (i.e., they don't know the information norms in a particular context). Furthermore, with the use of data mining and neural nets, even the people tracking do not know explicitly why some people are singled out for attention and others are ignored.

What is at issue here is the practices of organizations using personal information, and with data mining it is not just the fact that individuals often don't know that they are being tracked and monitored or don't know the information norms for particular contexts. Information gathered for one purpose is merged and mined to identify patterns of behavior that no individual could have imagined they were revealing when they (intentionally or unintentionally) disclosed information. Organizations gather information about lots and lots of people, merge the information, and "mine" it for patterns of behavior that are relevant to the organization's goals. Depending on the goal of the organization, individual customers, clients, or "persons of interest" are categorized into groups and the organization treats us as a member of the group. Scenario 4.3 illustrates just this.

Organizations have goals—be it a security agency screening an airline passenger list for potential terrorists or TechStation.com looking to increase its sales—and they want to achieve their goals efficiently. In theory, the more information they have about individuals, the better decisions they can make. IT tools have been developed to create and analyze personal information to help various organizations achieve their goals, and the reproducibility of IT makes it possible to collect an inordinate amount of fine-grained information and merge it with other data. Clickstream gives

Web-based companies information about how customers interact with their website, information they can use to maximize the likelihood of a visitor buying something. Data mining tools look for patterns in data that an organization might not even have thought would be relevant to their goals.

We should point out here that although we have suggested that organizations gather and process information in order to achieve their goals, information may continue to be collected even though it doesn't serve those goals. For example, although it is used abundantly in the UK, recent reports suggest that CCTV has very little effect on crime rates. As a *Guardian* reporter recently explained: "Massive investment in CCTV cameras to prevent crime in the UK has failed to have a significant impact, despite billions of pounds spent on the new technology . . . Only 3 percent of street robberies in London were solved using CCTV images, despite the fact that Britain has more security cameras than any other country in Europe." [http://www.guardian.co.uk/uk/2008/may/06/ukcrime1]

Whether an organization is interested in consumption, terrorist behavior, or employee productivity, the "name of the game" is *prediction*. Organizations want to predict how individuals are likely to behave and treat them accordingly. A bank may want to know the likelihood of you having enough money in the future to use their investment services. If you are likely to be a long-term, profit-generating customer, they may be willing to offer you lower interest rates on loans or higher rates on interest-bearing accounts. On the other hand, if you are not likely to earn enough money in the future to take advantage of their more profitable services, then the bank may be less interested in you; it may charge you a fee for your checking account while more desirable customers are offered free checking. Similarly, the airline security system is interested in knowing whether you fit the profile of a terrorist. They sort people in a variety of ways including by the ethnicity of names. Here we see how crude the sorting can be because the probability of someone with a Middle Eastern name being a terrorist is, no doubt, so small as to be insignificant but security agencies use it anyway.

Notice that there is a conundrum here. Although these practices may seem to make sense as a way of predicting behavior, they also fit the pattern of

prejudice and injustice insofar as individuals are being treated as members of a class—stereotypes—and not as individuals. The parallel between this social sorting and discrimination is well recognized and, in general, organizations avoid sorting individuals into categories such as race to avoid being accused of discrimination. Antidiscrimination laws apply to using race, gender, religion, and so on. Critics worry that even though these categories are avoided, the categories that are used indirectly lead to discrimination. Some of the literature in this area refers to this as "weblining" to show the parallel to "redlining," a practice in the insurance industry that was made illegal because it was so discriminatory.

Although the categories that organizations use often seem demeaning to individuals, the most significant criticism is that the sorting leads to inequality. Different categories of individuals are treated differently, and the differential treatment results in individuals having very different opportunities. Although this might be justified when we examine a particular context, the cumulative effects of social sorting may well be divided and segmented (if not caste-like) societies. If you fit one category, you are likely to: avoid the suspicion of law enforcement, find employment, travel without being harassed, borrow money with ease, obtain insurance, and receive preferential pricing and access. But if you fit a different category, your opportunities in all of these domains are likely to be diminished. As in our discussion of the panopticon, we see again how democracy may be undermined through these practices.

Crude Categories

To illustrate the problem further, it may be helpful to explore a radical idea. What would happen if the United States adopted legislation that prohibited organizations from using anything but the crudest (that is, broadest) categories? Suppose that all customers and clients had to be treated alike and no information could be gathered or used to sort individuals into categories. To be sure, this would create many problems but suppose it was, at least, the default position so that any organization that wanted to do otherwise had to petition an agency—call it the Category Agency—for permission to use other categories. How would this transform the flow of information?

Consider some examples. In political campaigns, information for potential voters would have to be targeted to all citizens; no distinctions could be made between citizens who lived in this or that district or who had this or that "demographic." All citizens would get the same information about candidates. Similarly, imagine that consumer-marketing firms would only be able to advertise to consumers, writ large; that is, they would have to send the same advertising to all consumers and air the same commercials in all regions of the country. Employers would have to give all employees the same benefits. Airlines would have to charge the same for a ticket from one place to another no matter who or where an individual bought a ticket.

A few advantages come immediately into view. The first, and perhaps too obvious one, is that individuals would have a good deal more privacy because there wouldn't be much fine-grained data gathered about them. There would be no use for it.

Second, individuals would be treated much more as autonomous beings. Instead of having their behavior watched with inferences made about who they are and what they want, individuals would have to be asked. That is, advertisements could be distributed and special discounts could be made, and individuals would respond—rather than their response being predicted. Surveys could be taken, but a wide spectrum of individuals would have to be surveyed and the results accumulated into one database that revealed "customer" attitudes. Individuals would, it seems, be treated as rational beings capable of thinking, processing information, and making judgments, rather than entities to be watched and manipulated. Indeed, in the process of getting information to individuals qua individuals (rather than to a category), we would all be exposed to a wider range of information—that was sent to everyone—and called upon to think about it.

Third, and related to the second point, individuals would be treated as changeable—because they have autonomy. In the fine-grained, predictive systems, organizations put us in a category and then feed us information accordingly. This makes us more and more what we already are. In a system of crude categories, individuals are exposed to a wide range of information and can do their own choosing and selecting, and over time may change their likes and dislikes, attitudes, and political beliefs. Perhaps ironically,

when we treat people equally, people are more likely to learn and to grow, and are *less* likely to become homogenous.

This proposal is not without drawbacks, but it adds to the picture of the importance of privacy in the sense that it shows us that when personal information is used the way it is being used now, individuals are treated as objects, not as persons—as means to the goals of organizations, not as ends in themselves (rational beings capable of making decisions for themselves).

Summary of the Arguments for Privacy and Against Surveillance

Returning to our broad analysis of privacy, where do we stand? We have seen that personal information flows intensively and extensively in IT-configured societies. The flow of information shapes organizational practices and these practices powerfully affect the lives and experiences of individuals. The effects of these practices have been framed as issues of privacy, but we have seen that privacy is an extremely complex idea and the effects of personal information gathering practices are multifaceted, touching on other values such as autonomy, equality, and democracy.

We don't claim to have figured out the entire privacy puzzle here. But we have identified a number of accounts of the value of privacy. When personal information flows as readily as it does in IT-configured societies, privacy protection is a daunting challenge. We turn now to consider some general strategies for privacy protection.

Is Privacy Over? Strategies for Shaping Data Flow

It is not uncommon to hear it said that "privacy is over; forget it." Such statements are usually followed by an explanation that there is just too much personal information available, and once it resides in a database anywhere in the world, it is impossible to control where it flows. Such statements are typically followed by an example of some form of personal information that we would want to be quickly and easily available—say you

are traveling away from home and are in a car accident. “Wouldn’t you want the medical staff to be able to get access to your medical records wherever they are?” Obviously, the answer is “yes.” However, saying “yes” to this question does not seem equivalent to saying we should let go of privacy altogether. Rather, the example suggests that in the domain of medical records, we want the norm of distribution to be such that medical professionals, or whomever we want, to be able to get access and as quickly as would serve our interests.

The “privacy is over” claim seems too glib and overly simplistic. Of course, there are many contexts in which personal information should be readily available to certain users. Nevertheless, there is too much at stake here to throw up our hands and give up on shaping the production and flow of personal information. Privacy issues can, and should, be framed as part of the larger enterprise of structuring and constituting democratic social institutions in IT-configured societies. This is a matter of strategy as well as specifying policies for particular domains.

Our analysis above has referred to a relatively small number of the issues that are currently being debated in the United States as well as other countries. The breadth and complexity of the issues can be grasped by taking a look at several key websites on the topic. We draw your attention in particular to the Electronic Privacy Information Center (http://www.epic.org), Privacy International (http://www.privacyinternational.org), the Electronic Frontier Foundation (http://www.eff.org), the Center for Democracy and Technology (http://www.cdt.org), privacy.org (http://www.privacy.org); and the Center for Digital Democracy (http://www.democraticmedia.org). These sites provide a wealth of information on current issues, proposed legislation, court cases in which privacy issues are being contested, and news alerts. The range of issues is illustrated, for example, by the list of current issues that appears on privacy.org:

Biometrics technologies
Video surveillance
Online privacy and e-Commerce
Workplace monitoring

Wireless communications and location tracking
Data profiling
Criminal identity theft
Background checks
Information broker industry
Public records on the Internet
Financial privacy
Medical records confidentiality and genetic privacy
Wiretapping and electronic communications
Youth privacy issues
Digital rights management
Digital television and broadband cable TV
Radio Frequency Identification (RFID)
Real ID
Absence of federal-level privacy protection law
Behavioral targeting

A review of the debates over these issues reveals some common strategies that are adopted or are being proposed across different contexts. Although not trying to be thorough, we will discuss several strategies that seem important for understanding privacy debates or taking action.

Fair Information Practices

A recurrent issue in privacy debates is whether sectors or industries should be regulated with respect to their personal information practices through legislation and penalties for failure to comply *or* should be allowed to self-regulate. Most industries prefer not to be regulated by the government. They claim that they know their domain better than the government and hence, know better how to encourage and achieve high standards of performance (in many different areas, including privacy). In self-regulation, an industry will gather its members, develop a set of rules or standards, and agree to abide by those standards. If all (especially the most powerful) members agree to abide by the standards, then the playing field is level and competition will not force a lowering of standards.

Often self-regulation works, and it works especially well when the interests of the industry and the interests of the public are aligned. On the other hand, when self-regulation doesn't work and the public or a set of customers or clients are not being served, regulation is necessary. In the case of privacy, at least in the United States, there is a mixture of self-regulation and legislation, although there is some indication that self-regulation doesn't work. Consider a 2005 report from EPIC entitled "Privacy Self Regulation: A Decade of Disappointment." In the report, EPIC entreats the Federal Trade Commission and Congress to "seriously reconsider its faith in self-regulatory privacy approaches. They have led to a decade of disappointment; one where Congress has been stalled and the public anesthetized, as privacy practices steadily worsened." EPIC calls for the government to "create a floor of standards for protection of personal information based on Fair Information Practices."

We do not want to engage in the debate over self-regulation here. Whether there is self-regulation or legislation, a set of general principles are commonly used, either as the basis for structuring legislation or for specifying self-regulatory standards. The "Code of Fair Information Practices" was developed and recommended for implementation in the 1973 Report of the Secretary of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems (titled "Records, Computers and the Rights of Citizens"). Although it was never made into law, it has served as a model and been influential in the development of privacy policy. The Code specifies that: (1) there must be no personal data record-keeping system whose very existence is secret, (2) there must be a way for an individual to find out what information about him or her is in a record and how it is used, (3) there must be a way for an individual to prevent information about him or her that was obtained for one purpose from being used or made available for other purposes without his or her consent, (4) there must be a way for an individual to correct or amend a record of identifiable information about him or her, and (5) 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 the misuse of data.

To see how these principles have been interpreted today, consider the following statement that appears on the website of the Federal Trade Commission (http://www.ftc.gov):

> Over the past quarter century, government agencies in the United States, Canada, and Europe have studied the manner in which entities collect and use personal information—their "information practices"—and the safeguards required to assure those practices are fair and provide adequate privacy protection. (27) The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices. (28) Common to all of these documents [hereinafter referred to as "fair information practice codes"] are five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.

Other examples of the code can be found on the Web. For example, on the website of the Center for Democracy and Technology you will find "Generic Principles of Fair Information Practices that include Principles of Openness, Individual Participation, Collection Limitation", Data Quality, Finality, Security, and Accountability [http://www.cdt.org/privacy/guide/basic/generic.html]

Thus, fair information practices might be understood as the starting place for thinking about privacy policy. However, although the principles are recognized, they have not been uniformly interpreted or implemented. Information collected for one purpose is often used for other purposes, for example, when grocery stores sell information from their loyalty cards to advertisers. In Scenario 4.1, we see that e-mail (which we might not even think of as information) is scanned for advertising purposes. Another area of slippage from the intention of the Code is the right of individuals to access personal information held in databases. Although this right may exist in theory, most of us have no idea where information about us resides and how we would go about getting access to that information, or how we could correct the information if it were erroneous.

Transparency

A review of recent debate on privacy issues suggests that a common approach being proposed is the adoption of transparency policies. One of the reasons that consumers and clients are so compliant when it comes to their privacy is that they are unaware of information practices. For example, most of those who shop online are unaware that their clickstream is being tracked and this information is being put into a pool of other data. Most Gmail users are unaware of content scanning.

Transparency would go a long way toward finding out exactly what citizens, clients, and consumers think about information practices. Earlier in this chapter we examined the claim that people don't value privacy. There we noted that because the public knows so little about information practices, we cannot say whether most people care or don't care about who has their personal information and how it is used. Making these practices transparent would be a good first step in finding out what the public really thinks about privacy.

Opt-In versus Opt-Out

Another general approach is to insist on opt-in rather than opt-out policies. This has been a topic of dispute in a recent discussion of telephone records. Evidently, the Federal Communications Commission and the National Cable and Telecommunications Association are scrabbling over whether records of whom we call should be an opt-in or opt-out. [See www.epic.org]

The opt-in versus opt-out decision was also a factor in the controversy over Facebook's Beacon program. Mentioned earlier, this was Facebook's advertising program that announced to one's friends what one had just bought. For Facebook this was an advertising schema. They could collect revenue from the companies for advertising purchases from them. Facebook users reacted with anger. As Mark Zuckerberg (CEO of Facebook) explains: "The problem with our initial approach of making it an opt-out system instead of opt-in was that if someone forgot to decline to share something, Beacon still went ahead and shared it with their friends." [http://blog.facebook.com/blog.php?post=7584397130]

The opt-in rather than opt-out strategy goes hand in hand with transparency. Indeed, given how little information consumers, clients, and citizens have about information practices, the opt-out strategy seems unfair if not deceptive. Personal information is gathered and used and if we figure out what is happening we can optout. By contrast, if organizations cannot use personal information about us unless they get our permission, then they have to inform us of their practices and convince us that we want to opt-in. This is consistent with our analysis above insofar as opt-in treats us as rational beings capable of making decisions, rather than passive objects to be manipulated.

Design and Computer Professionals

Rarely mentioned although sometimes implicit, we would like to call attention to the role that IT professionals can play in protecting privacy. The architecture of IT systems can make a big difference in what kind of data is collected and how it flows from place to place. This is the business of IT professionals. Chapter 7 is devoted to a discussion of IT professionals and their responsibilities, but here we want to note that they can play a role in protecting privacy in several important ways. IT professionals could collectively make a commitment to protecting privacy similar to the commitment that environmental engineers seem to adopt with respect to protection of the environment. This is not a farfetched idea because the original ACM (Association for Computing Machinery) Code of Professional Conduct (passed by the ACM Council in 1973) specified that: An ACM member, whenever dealing with data concerning individuals, shall always consider the principle of the individuals' privacy and seek to:

- Minimize the data collected
- Limit authorized access to the data
- Provide proper security for the data
- Determine the required retention period of the data
- Ensure proper disposal of the data

When the code was revised in 1992, these edicts were dropped and replaced with a General Moral Imperative specifying that an ACM member will "Respect the privacy of others." The Guidelines explain that: "It is the

responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals."

Individual IT professionals can make a difference both in the way they design systems and in the way they present and discuss decisions with their clients. Because of their special expertise, IT professionals are often in the best position to evaluate the security and reliability of databases of personal information, and the potential uses and abuses of that information. Thus, they are in a position to inform their clients or employers about privacy issues and to participate in public policy discussions. In particular, because IT professionals understand how IT systems work better than anyone else, they can use their expertise to encourage practices that safeguard privacy.

Personal Steps for All IT Users

Several of the websites we mentioned above provide recommendations for individuals and what they can do to protect themselves. EPIC provides a list of links to tools that one can use to send e-mail anonymously, surf the net anonymously, or make sure that one's computer is secure. The Center for Democracy and Technology's Guide to online privacy lists ten ways to protect privacy online:

1. Look for privacy policies on the Web.
2. Get a separate e-mail account for personal e-mail.
3. Teach your kids that giving out personal information online means giving it to strangers.
4. Clear your memory cache after browsing.
5. Make sure that online forms are secure.
6. Reject unnecessary cookies.
7. Use anonymous remailers.
8. Encrypt your e-mail.
9. Use anonymizers while browsing.
10. Opt-out of third-party information sharing. [http://www.cdt.org/privacy/guide/basic/topten.html]

The Electronic Frontier Foundation also has a list of twelve ways to protect your online privacy:

1. Do not reveal personal information inadvertently.
2. Turn on cookie notices in your Web browser, and/or use cookie management software or infomediaries.
3. Keep a "clean" e-mail address.
4. Do not reveal personal details to strangers or just-met "friends."
5. Realize you may be monitored at work, avoid sending highly personal e-mail to mailing lists, and keep sensitive files on your home computer.
6. Beware of sites that offer some sort of reward or prize in exchange for your contact information or other personal details.
7. Do not reply to spammers, for any reason.
8. Be conscious of Web security.
9. Be conscious of home computer security.
10. Examine privacy policies and seals.
11. Remember that YOU decide what information about yourself to reveal, when, why, and to whom.
12. Use encryption!

These lists and advice are relevant to taking an ethical stance. If an individual values privacy, both on an individual level and as a broader social good, then there are personal actions that can be taken to enhance individual privacy. If enough individuals protect their own privacy diligently, a society's overall privacy is enhanced. This kind of individual and collective action is an alternative to the "it's over—privacy is passé" argument described above. Individuals convinced that privacy does matter do not have to passively accept the status quo. In this way, an ethical analysis of the value of privacy leads to actions that resist information intrusions.

A Note on Privacy and Globalization

Finally, the many and complex issues of privacy that we have been discussing arise in the context of an increasingly globalized economy. This means that personal information flows across national borders. Yet privacy

laws vary from country to country. It is a complex and delicate issue as to what happens to personal data when it moves from one place with one set of laws to another place with a different set of laws. Many questions arising from this situation have yet to be settled.

Conclusion

Privacy may be the single most important facet of the ethical issue surrounding IT. We have tried to show this by making clear the importance of privacy to democratic society and the subtle ways in which our lives are changed when we are being watched. Individuals who walk through life knowing that each step creates a digital record that may haunt them for years differ significantly from individuals who walk through life confident that they live in an open society in which the rules are known and fair. It is sobering to think about which kind of persons we have become in the last two decades.

Protecting personal privacy is not easy and is not likely to get easier. The most effective approach to privacy protection requires action on several fronts. One thing is for sure: The use of personal information is not going to diminish of its own accord. Information about individuals is extremely valuable both in the private and public sector. Individuals may not realize how valuable that information is, or how much is at stake if privacy is lost. It will take a concerted effort from individuals and organizations to reverse, or at least confront, the loss of privacy that has accompanied the growth of IT.

Study Questions

1. What are the significant differences between personal information flow with IT and personal information flow without IT?
2. What are three arguments that can be made for why we shouldn't worry about privacy? How can each of the three be countered?
3. Explain Rachels's argument that privacy is necessary for a diversity of relationships.

4. What does gossip have to do with privacy?
5. Nissenbaum's account of privacy as contextual integrity explains privacy in terms of two norms. Explain, and give two examples of each type of norm. Choose examples that show how the norms vary from context to context.
6. What is the panopticon? How do prisoners experience themselves differently when they are in panopticon prisons?
7. What happens to people who are watched all the time according to Reiman?
8. Pick a domain of human activity in which information about individuals is gathered (e.g., insurance, buying, political campaigning, and fund-raising), and describe how organizations in that sector sort individuals into categories and try to predict their behavior.
9. What would be the benefits and drawbacks of limiting organizations to using only crude categories in their information-gathering practices?
10. What are the five principles of the code of fair information practices?
11. How would transparency policies protect privacy?
12. What is the difference between opt-in policies and opt-out policies?
13. What do you think are the three most significant personal steps an individual can take to protect his or her personal information?