CHAPTER

10

The Digital Divide, Democracy, and Work

LEARNING OBJECTIVES

Upon completing this chapter, you will successfully be able to:

- Explain what is meant by phrase *digital divide* and why this "divide" is morally significant at the global as well as local levels,
- Describe key strategies and policies proposed by the Web Accessibility Initiative (WAI) to make access to cybertechnology more accessible to disabled persons and groups,
- Articulate key issues affecting cybertechnology and race, as they apply both to technology–access affecting racial and minority groups (in the United States and globally) and the use of the Internet to reinforce racism,
- Assess the impact that cybertechnology has had for gender issues, particularly as they apply to concerns about access to high-tech jobs for women and to gender bias in software design,
- Describe the many ways in which cybertechnology can both enhance and threaten democracy, as well as democratic values and ideals,
- Understand the impacts that cybertechnology has had for employment and work in the twenty-first century, both in terms of the *transformation* of work and the *quality* of work life.

Unlike Chapters 5–9, which focused on the impacts that cybertechnology has for specific moral, legal, and social problems—namely, privacy, security, crime, intellectual property, and Internet regulation—This chapter considers the impacts that this technology has for a wide range of issues that cut across three broad (social) categories:

- *Sociodemographic groups* (affecting social/economic class, race, and gender)
- *Social and political institutions* (such as education and government)
- *Social sectors* (including the workplace)

A common characteristic unifies the otherwise disparate issues examined in this chapter: They are often approached from the perspective of *sociological/descriptive ethics*. Recall that in Chapter 1 we drew a distinction between descriptive and normative approaches to the study of moral issues, noting that while social scientists conduct research that is essentially

designed to report (or describe) sociological aspects of cybertechnology, those aspects often have normative implications as well. In this chapter, we examine some issues primarily from the vantage point of descriptive ethics, especially as they require an analysis of statistical and empirical data. In other cases, we also examine normative aspects of those issues. The latter perspective is particularly apparent in our analysis of concerns involving social equity/access to digital technology. We begin with a scenario that briefly illustrates a cluster of issues examined in greater detail in later sections of this chapter.

▶ **SCENARIO 10–1:** Digital Devices, Social Media, Democracy, and the "Arab Spring"

In early 2011, large political protests erupted in many Arabic-speaking countries in North Africa and the Middle East—including Egypt, Tunisia, Libya, and Yemen—where protestors, many of them young persons, demanded governmental reforms. In Egypt, for example, protestors used social media sites, accessible via their mobile devices, to organize demonstrations in Cairo. Subsequently, the government led by then President Hosni Mubarak soon fell (as did the ruling governments in Tunisia, Libya, and Yemen). This political uprising, bordering on what some describe as a "revolution," has since been described by many journalists and media outlets in the West as the "Arab Spring." Many optimists, especially in the West, believed that a wave of democratic governments would soon emerge across the Arab world.[1] Even though that outcome has not been realized (at least not so far), organized protestors were nevertheless able to topple the regimes of powerful governments in the Arab world—something that would have seemed unthinkable just a few years before. ■

In the past, political regimes in the countries that were affected in this region of the world were able to squash political protests by preventing the mobilization of their citizens into large-scale demonstrations and rallies. So, one might naturally ask: What was so different in the Arab Spring movement, and why did it succeed (at one level, at least, even if no democratic governments have yet taken hold in these countries)? Although many of the political leaders, including the Mubarak administration in Cairo, had reacted immediately to the protestors by shutting down the country's Internet services and mobile phone resources, their actions were too late. The protestors in Egypt, anticipating the government's reaction in advance, had already unified and planned out their organized demonstrations via social media sites such as Facebook and Twitter before the online services in Egypt were able to be shut down. So it would seem that these protestors' success in bringing down a powerful government could be attributed, in large part, to their adept use of electronic devices and online social media to organize their large demonstrations.

Historically, many governments have taken advantage of the latest technologies in ways that have enabled them to remain in power by controlling their citizens; for example, some governments have used surveillance technologies to monitor the movements of their citizens, thereby making it very difficult for them to mobilize. Also, some governments have used these technologies to eavesdrop on citizens and to intercept communications among dissenters and protestors. So the myriad uses of technology in the political/governmental sphere had often seemed one sided—that is, favoring the interests of those political regimes already in power. During the Arab Spring, however, ordinary citizens, including the protestors and their sympathizers, were able to turn the tables and use the latest technologies available to them (e.g., mobile phones, digital devices, etc.) and social media services (such as Twitter and Facebook) to bring down some firmly entrenched (and what many would also describe as "repressive") political regimes.

The purpose of Scenario 10–1 was not to provide a detailed analysis of the Arab Spring. Rather its objective was to get us to begin thinking about the relationship between technology and government in general, and technology and democracy in particular. One question this scenario might also cause us to consider is: How different would the political outcome in Egypt (and the other affected governments in North Africa and the Middle East) likely have

been if ordinary citizens, or even specific groups/classes of citizens, in those countries were not able to afford or to access the kinds of digital technologies they used? So it would seem that issues concerning democracy (and democratic forms of government) are now becoming increasingly intertwined with issues involving a government's policies affecting (affordable) access to digital technologies for all of its citizens.

We examine some access-related issues affecting specific demographic groups in Sections 10.1–10.4 in our analysis of the digital divide (socioeconomic class), disabled persons, racial minorities, and women, respectively. Concerns associated with the impact of cybertechnology on our political/social institutions are considered in our discussion of democracy and the Internet in Section 10.5, whereas cybertechnology-related issues impacting the contemporary workplace (as a social sector) are examined in Section 10.6.

▶ 10.1 THE DIGITAL DIVIDE

What, exactly, is the digital divide? Compaine (2001) suggests that the phrase *digital divide* is basically a new label for an earlier expression used to describe the "information haves and have-nots." He defines the digital divide as the gap, or "perceived gap," between those who have and do not have access to "information tools." According to Himma and Bottis (2014), however, this "divide" or gap can be more accurately understood as a "series of gaps" affecting the technological haves and have-nots. For example, there are gaps between those have and do not have digital devices and Internet access and also gaps (or divisions) between those who have and do not have the knowledge and ability to use digital tools (and thus enjoy their benefits). So, the digital divide refers not only to a division or gap affecting mere access to information technology; it also reflects, as Ryder (2015) points out, the significant gap between those who can and those who cannot "effectively benefit" from that technology.[2]

For our purposes, issues affecting the digital divide can be organized into two broad categories: the divide *between* nations and the divide *within* nations. The division between information-rich and information-poor nations is sometimes referred to as the "global digital divide"; the technological divides within nations, on the contrary, typically exist between rich and poor persons, racial majority and minority groups, men and women, and so forth. We begin with a look at the global digital divide.

10.1.1 The Global Digital Divide

Consider some statistics ranging from 2000 to 2014. In 2000, it was estimated that 361 million people, approximately 5.8% of the world's population, were online; the vast majority of those users lived in North America and Europe.[3] Since then, global Internet usage has expanded significantly. In June 2014, it was estimated that there were slightly more than three billion Internet users.[4] A significant shift had already occurred by 2005 when the list of countries or regions where more than 50% of the population used the Internet had grown to 30.[5] That year, seven nations—Australia, Canada, Japan, South Korea, Taiwan, the United Kingdom, and the United States—had an Internet penetration rate of higher than 60%.

As of 2014, the disparity between the percentage of Internet users in developed and developing countries continues to be significant. In India, for example, the penetration rate for Internet users is 15.8%, while in the United Kingdom, it is 89.8%.[6] The disparity is especially apparent when viewed from the perspective of continents or world regions. For example, in Africa (which includes approximately 15% of the world's population), the Internet penetration rate is 26.5%, whereas in North America, the Internet penetration rate is 87.7% (as of June 2014). On a positive note, however, the Internet usage growth in Africa was 2,527.4% between 2000 and 2011.[7] So, one might be encouraged by some reports describing the growth

in Internet usage at the global level. Yet, despite the progress that has been made in the African continent, critics worry that much more work still needs to be done to narrow, and perhaps one day even bridge, the global divide.

One obstacle to eliminating the global digital divide altogether is that developing countries struggle with low literacy rates; many people in developing nations cannot read and write in their native language, let alone in English. And much of the material on the Internet is in English. This has influenced advocates for improved Internet service for global users to lobby for the development of Web applications that include more graphics and images that can serve as universal symbols. (We return to this point in our discussion of technology-related access issues affecting disabled persons, in Section 10.2.) However, O'Hara and Stevens (2006) note that regardless of whatever explanation we give for the perpetuation of a global digital divide, one thing is patently clear: Inequalities regarding access to cybertechnology are closely tied to "economic inequality."[8]

10.1.2 The Digital Divide within Nations

Many developed nations still have significant divides within them regarding access to cybertechnology. For example, O'Hara and Stevens point to one such discrepancy in the United Kingdom. They note that in 2004, approximately one-half of all households were online, while only 3% of the poorest households were included in this number. As one might expect, there are also significant disparities within some developing nations as well. And in rapidly developing countries like India, the divisions that currently exist may eventually deepen. Consider that a growing segment of India's population is fluent in English and has the technical literacy required to work on many of the highly skilled jobs outsourced there; those on the other side of the divide, comprising the majority of the population of India, tend to have a low level of literacy and little or no access to digital/cybertechnology.

Some countries, including the United States, have instituted specific strategies designed to bridge the divide within their national borders. In response to concerns about the gap that existed in America in the early 1990s between those with and without access to computers, the Clinton administration initiated the National Information Infrastructure (NII) to ensure that all Americans would have access to information technology. To accomplish this objective, the National Telecommunications and Information Administration (NTIA) conducted a series of studies that investigated computer use among various groups.

One question that arose from the NTIA reports was whether a *universal service* policy was needed to ensure that all Americans have an appropriate level of access to Internet technology. Universal service policies have been controversial because they require subsidies, which often result either in user fees or higher taxes. However, proponents of a universal service policy for the Internet have pointed to the model that was used to subsidize telephone technology when that became available in the early part of the twentieth century. Without some kind of government-supported subsidy, people living in less-populated rural areas would not have been able to afford this new technology. So the U.S. Congress passed the Communications Act of 1934, which distributed the cost for telephone service in a way to make it affordable to all Americans. Today, the question is whether Internet access should be subsidized in a similar manner. In the case of telephone technology, arguments were made that having a telephone was necessary for one's well-being. Can the same argument be made in the case of digital/cyber technology and Internet access?

As we saw in Chapter 9, subsidies in the form of "E-rates" (i.e., federal technology discounts) have helped to defray the cost of Internet access for public schools and libraries in the United States. Unlike universal service policies involving telephones, which are aimed at subsidizing residential telephone service, E-rates for Internet access apply only to "community

points of access" such as public libraries. While E-rates may support universal Internet *access*, they do not provide universal Internet *service*. So, critics such as Chapman and Rotenberg (1995) have argued that merely providing community points of access to the Internet would be similar to a policy that simply placed telephones in public locations rather than making telephone service affordable for all Americans.

Some critics worry that the absence of a (universal) Internet service policy in the United States could adversely affect school-age children in low-income families. Consider the following scenario where someone tries to convince you that an Internet service policy is needed to level the playing field for economically disadvantaged students attending U.S. public schools.

▶ **SCENARIO 10–2:** Providing In-Home Internet Service for Public School Students

Sara, an advocate for disadvantaged youth in low-income families in America, asks you to review a short editorial she is preparing for a blog (dedicated to education-related issues). In that editorial, she argues: There are several reasons why the U.S. government should provide in-home Internet service for all students (Grades 1–12) whose families cannot afford to pay for it. First, the federal government mandates that all school-age children (of U.S. citizens) receive a free public school education. Second, the government is required to provide those children with the resources they need to complete their education (i.e., classrooms, labs, textbooks, etc.). Today, having in-home Internet service is a critical resource for students to be able to complete their homework assignments. School-aged students whose families cannot afford in-home Internet service are at a significant disadvantage in competing in the educational system. So, students whose families cannot afford the cost of in-home Internet service should have that service subsidized by government funding. ■

Is Sara's argument convincing? One might initially be inclined to object by noting that these students could go to public libraries to get the online resources needed to complete their homework assignments. However, Sara could reply that libraries are mere "points of access" (as noted above) and thus do not provide the kind of (universal) service needed by these economically disadvantaged students. Furthermore, Sarah might note that if we adopt the rationale used in her critics' objection, we should also require students to go to libraries to get the textbooks needed for their homework assignments as well, rather than having schools freely provide students with these resources. For example, she might invoke the following analogy: Because textbooks, like home Internet access, are essential resources for students completing their homework assignments, the same policies should apply for textbooks as for Internet access. But it is unlikely that Sarah's opponents would want to eliminate free textbooks for school-aged children.

Two points in Sara's argument are also worth reiterating. First, she is not advocating (government subsidized) universal Internet service at home for *all* school-aged children; rather, this subsidy would apply only for those students in families below a certain economic/income threshold. Second, this subsidized (Internet) service would apply for those eligible school-age children only while they are students and only during those periods of the year when they are actually in school; in other words, there would be appropriate constraints, especially in the form of time limitations, for this Internet service policy.

It would be interesting to evaluate Sara's argument via the seven-step strategy described in Chapter 3 to see whether it satisfies the requirements for being both valid and sound. Of course, even if the argument can be shown to be valid, that is, merely in virtue of its logical form, one could still ask whether the premises are all empirically true. Assuming that they are, we could also ask whether a key claim made in this argument—namely, that school-age children in families unable to afford in-home Internet service are at a significant disadvantage in competing in the educational system—describes an issue that is fundamentally *ethical* in nature.

10.1.3 Is the Digital Divide an Ethical Issue?

What does it mean to say that the digital divide is an ethical issue? Is every kind of divide regarding unequal access to goods and services necessarily an ethical problem? Some skeptics have pointed to the divide between those who have and do not have Mercedes-Benz automobiles, arguing that there is a "Mercedes-Benz divide" and that many of us fall on the "wrong side" of it; they also correctly note that this kind of divide is not an ethical issue. But we could respond to these skeptics by pointing to the divisions that exist between those who do and those who do not have access to vital resources such as food and healthcare—divisions that many ethicists believe raise questions affecting the just distribution of primary goods and resources. So, how should we view unequal access to cybertechnology? Is it closer to the Mercedes-Benz divide, or is it closer to divisions involving access to food and healthcare?

Distributive Justice and Access to Vital Human Resources

As suggested above, some question whether the digital divide raises concerns affecting distributive justice. But what do we mean by "distributive justice," especially in the context of cybertechnology? According to van den Hoven and Rooksby (2008):

> Distributive justice in contemporary information societies concerns, among other issues, the distribution of information, information services, and information infrastructures.[9]

The authors note that while there has been much enthusiasm about the emergence of new technologies, there is also concern over "the uneven distribution of the new information wealth, both within nations and internationally."[10] To argue that the unequal distribution of information wealth is a moral issue would require that we show that information is a kind of "primary good" that is vital for human flourishing. So, we need to consider whether information meets the criteria of a kind of good or resource that is *vital* for one's well-being. Additionally, if we can show that not having access to cybertechnology either denies or unfairly limits access to information or to certain kinds of basic goods—what Moor (2004) calls "core goods" (or "core values"), such as knowledge, ability, freedom, and so forth—then we can make a fairly strong case that unequal access to cybertechnology is a moral issue affecting distributive justice.

In his classic work, *A Theory of Justice*, philosopher John Rawls introduces the notion of *primary social goods*, which are resources that satisfy basic human needs and thus have a special value or "moral weight" in society. Rawls notes that with these goods, humans "can generally be assured of greater success in carrying out their intentions and in advancing their needs."[11] Van den Hoven and Rooksby argue that Rawls' theory of justice in general, and his notion of a primary social good in particular, can be extended to include "information goods." They further argue, however that a "fully fledged theory of justice that takes adequate account of the new information goods" still needs to be fleshed out.[12] In the meantime, however, we can examine some recent models that have been advanced to show why the digital divide is indeed a moral issue affecting distributive justice.

One model has been articulated by Moss (2002) who argues that persons lacking access to cybertechnology are deprived of resources that are *vital for their well-being*. He points out that without access to cybertechnology, people are unfairly disadvantaged because their:

1. Access to knowledge is significantly lessened or prevented.
2. Ability to participate fully in the political decision-making process and to receive important information is greatly diminished.
3. Economic prospects are severely hindered.[13]

First, Moss claims that people who are deprived of access to cybertechnology are not able to benefit from the increasing range of information available on the Internet and thus are

falling further behind in the information era. Second, because of political barriers to participation in the decision-making processes in developing countries, people in remote areas without access to the Internet may have no means at all of participating in national debates or of receiving information about important developmental matters and policies that can significantly affect them. Third, Moss believes that because so much economic growth is driven by the information and communication sector, people living in countries that are not part of this sector are disadvantaged.

With regard to Moss's second and third points, Norris (2001) makes a similar observation by noting that "the underclass" of information poor may become "further marginalized" because they will lack the skills needed both for "civic engagement" and economic success. Norris also worries that because people in this group will not possess essential computer-related skills, they will not be able to enjoy the kinds of good careers made possible by "educational opportunities."[14]

In response to advocates like Moss and Norris, however, one could argue that some people (and some nations) have always been disadvantaged in accessing new technologies such as automobiles, household appliances, and so forth. But, once again, we can respond by pointing out that this kind of criticism misses a crucial point. As we have noted, disparities in access to certain technologies and goods, such as Mercedes-Benz automobiles, do not in themselves constitute an ethical issue. We should also point out that divisions of this type are generally accepted in capitalist societies. However, if Moss's thesis about why cybertechnology is important is correct, then having access to cybertechnology is essential for one's *well-being* in ways that having access to other kinds of technologies—for example, "discretionary technologies" that provide convenience and entertainment—is not. So, one question that arises is: Do we have a moral obligation to bridge the digital divide? And if we do, are affluent nations the ones responsible for bridging this divide?

Making the Case for a Moral Obligation to Bridge the Digital Divide

Bottis and Himma (2008), in presenting their argument for the view that "affluent nations" have a moral obligation to bridge the divide, begin by clarifying some important points. For example, they note that we first need to draw a critical distinction between saying that "X is a good thing to do" and saying that "we are obligated to do X." Bottis and Himma believe that most people would likely agree that eliminating the digital divide would be a good thing to do; they also suggest, however, that there would likely be far less consensus as to whether we (i.e., some affluent nations) have an obligation to do it.

Bottis and Himma point out that one's failing to do something morally good is not necessarily morally wrong; they use the example of someone's risking his or life to save a person caught in a fire in a building. Failure to risk one's life to save another here, they correctly note, is not something that necessarily merits either blame or punishment. Of course, the act of attempting to save someone's life in the fire would be a good thing, but (assuming that you and I are not firefighters) we are not morally obligated to do it. Doing an act such as that crosses over to a category that philosophers and ethicists call "supererogatory." That is, the act of risking one's life in a fire to save another is morally good but is also "beyond the call of moral obligation." Bottis and Himma also note that we "praise supererogatory acts, but not obligatory acts" and we "blame nonperformance of obligatory acts, but not supererogatory acts."[15] So in this scheme, should we view the act of bridging the digital divide as a supererogatory act, in which case we are not morally obligated to do anything?

Himma (2007) points out that because many people believe that we are morally obligated only to do no harm, they infer that we have no obligation to bridge the digital divide. But he also believes that such a view is "inconsistent with the ethics of every classically theistic religion as well as our ordinary intuitions, as well as classic theories of deontology and consequentialism." In the case of deontology, for example, Himma notes that virtually all deontological

theories hold that we "have an obligation to help the poor."[16] For example, he points to the *prima facie* obligation of *beneficence* that we have to help those in need, as implied in Ross' deontological theory. (You may wish to review Ross' ethical theory of act deontology described in Chapter 2.)

In Chapter 2, we saw that contract-based ethical theory holds that while we are morally obligated to "do no harm," we have no explicit obligation to do good—in this case, no moral obligation to bridge the digital divide. According to this view, we are behaving morally as long as we do nothing to prevent others from acquiring cybertechnology and Internet access. But is this minimalist view of morality adequate? Recall that in our discussion of contract-based ethical theories in Chapter 2, we saw that individuals and nations have a moral obligation to do good (to others) only in cases where individuals or nations have an explicit contract in which they are required to come to the aid of others. However, we also saw that there are some compelling reasons to be skeptical about such a limited theory of moral obligation.

In our critique of contract-based ethical theories, we saw that a more robust theory of morality requires that we come to the aid of those who are in danger of being harmed, whenever it is in our power to do so. For one thing, we saw that doing this could help to make cyberspace a safer place, especially for those individuals and groups vulnerable to online harm. And we can construct an analogous argument to show why coming to the aid of other kinds of vulnerable (or at least disadvantaged) individuals and groups—that is, those without Internet access—would also be the right thing to do. If Moss is correct in claiming that access to cybertechnology is vital to one's well-being, then is it plausible to suggest that we have at least some obligation to provide access to those who are disadvantaged?

▶ 10.2 CYBERTECHNOLOGY AND THE DISABLED

Not only do equity-and-access issues involving cybertechnology affect poor people in developing nations and people in low-income groups within developed nations, they also affect many disabled people. So, some suggest that core equity-and-access issues underlying the digital divide apply to this group of people as well. There has been much discussion about implementing strategies and policies to make the Internet and digital technologies more accessible to disabled persons. Tim Berners-Lee, director of the World Wide Web Consortium (W3C) and the inventor of the HTTP protocol that underlies the Web, has stated, "The power of the Web is in its universality. Access by everyone regardless of disability is an essential aspect."

The W3C was formed, in large part, to promote standards that ensure universal Web access. It established a Web Accessibility Initiative (WAI), which has produced guidelines and protocols for developing software applications that improve access for disabled persons. These applications range from software used in speech synthesizers and screen magnifiers to proposed software applications that will benefit people with visual, hearing, physical, cognitive, and neurological disabilities.[17]

WAI representatives have worked with industry groups and governmental organizations to establish guidelines for the design of "user agents," which are intended to lower barriers to Web accessibility for people with disabilities. These user agents include Web browsers and other types of software that retrieve and render Web content; the agents are designed to conform and communicate with other technologies, especially "assistive technologies" such as screen readers (which perform a function similar to Braille applications in offline contexts). Grodzinsky (2000) argues that computers equipped with assistive technologies and "adaptive devices" can be "equalizers" in the era of information technology because they enable people with disabilities to participate in and compete for jobs in the contemporary workplace.

Some critics might ask why we should continue to fund initiatives such as WAI, especially because of the financial commitment involved and because disabled persons comprise a relatively small portion of the overall population. In response to those critics, WAI proponents such as Asakawa (2012) argue that access to technology is not simply a privilege but rather a "human right." Other WAI supporters, however, take a different tack in pressing their case for why initiatives for the disabled should continue to be supported. For example, they point out that some measures taken for the disabled have had positive outcomes for other groups, especially poor people who are often forced to deal with literacy problems and inadequate equipment. It may well turn out that voice-recognition technology designed to assist disabled persons who are unable to use keyboards will ultimately also benefit nondisabled persons with low literacy skills. So we see that larger groups of (nondisabled) people have benefited and could continue to benefit from some Web-based initiatives designed for disabled persons, even though the resulting positive effects in the past may have been unanticipated and unintended.

We can also point to an example of an accessibility-related initiative in the nondigital world that was intended to accommodate disabled persons yet has benefited the public in general. Ramps designed for wheelchair accessibility have not only benefited people in wheelchairs but have also been very useful to nondisabled persons as well, such as parents pushing baby carriages. Also, consider some of the advantages that sloped curbs on street corners have provided many nondisabled persons—bicyclists and skaters have benefited from these features, which were initially intended to serve disabled persons (Woodbury 2002). So, many of WAI's proponents argue, analogously, that ordinary users will likely continue to benefit from the computer design enhancements to user interfaces that are initially intended to assist disabled persons.

Because improving access to cybertechnology for the disabled has potential benefits for society as a whole, we can formulate a utilitarian argument to advance this cause. However, we should also be cautious about extending this argument too far. What would happen if, in the future, the broader population did not realize any benefits from improving access to cybertechnology for the disabled? Could this kind of outcome lend support to a utilitarian argument against investing in initiatives that improved access for the disabled? After considering this, you can better understand some of the possible dangers of relying too heavily on utilitarian principles when advancing a moral argument for improved access for the disabled.

We conclude this section by noting that there are additional concerns affecting cybertechnology and the disabled that are unable to be examined here. Our main objective in this section, however, was to identify and briefly describe some key issues and concerns involving the ongoing debate about which kinds of initiatives ought to be implemented to improve cybertechnology access for disabled persons. Next, we examine the impact of that technology for racial minorities.

▶ 10.3 CYBERTECHNOLOGY AND RACE

We have seen that even in developed countries like the United States, many lower-income individuals and families still do not have in-home Internet access; not surprisingly, many of these individuals also belong to racial and ethnic minority groups. In this section, we examine race-related issues affecting cybertechnology from two distinct perspectives:

1. Statistical data concerning Internet usage patterns of racial minority groups
2. The role(s) that the Internet can play in either exacerbating or reducing racism

We begin our analysis with a brief discussion of (1).

10.3.1 Internet Usage Patterns

Consider some statistics ranging from 2000 to 2011 that correlate income (social class) and race with the digital divide in the United States. In 2000, 51% of all homes had at least one computer, and 41.5% of all homes had Internet access. In terms of income, 86.3% of households earning more than $75,000 per year had Internet access, while of those households earning below $15,000 per year, only 12.7% had access. From the vantage point of race, 46.1% of white Americans and 56.8% of Asian Americans had access, contrasted with only 23.5% of African Americans and 23.1% of Hispanics who did.[18]

By 2008, 73% of adult men and women in the United States had Internet access at home, while 90% of young people between the ages of 18 and 29 used the Internet. However, the penetration rate for black Internet users in the United States then was 59%, which was still well below the penetration for the American population as a whole.[19] In 2011, however, statistics for African American vs. white users changed significantly. Whereas Internet usage among whites was estimated to be 88%, the rate of African Americans using the Internet had grown to 80%. Perhaps even more interesting was the rate at which the use of access to broadband Internet connection had grown for African Americans. Whereas 65% of African American Internet users had broadband access, only 53% of white American Internet users enjoyed this service; nearly half of these users had not migrated from earlier forms of Internet access such as dial-up technologies.[20]

Yet, despite the gains made by African Americans (vis-à-vis their white counterparts) regarding Internet use, some significant differences in usage patterns between the two groups continue to persist. For example, Burn (2011) notes that whereas 26% of white Americans used the Internet for entertainment purposes, 68% of African Americans used it for this purpose. African American Internet users also used the Web more frequently than white users for activities such as news, health, and sports.

Our analysis of technology and race thus far has focused primarily on statistical data pertaining to racial groups—mainly African Americans—with regard to levels of Internet access. We have not yet considered other kinds of technology- and race-related questions. For example, have Internet-based technologies exacerbated racism? Or, have they helped to reduce—or possibly even eliminate—racism? While one might initially be inclined to assume the latter to be true, we need to question that assumption.

10.3.2 Racism and the Internet

Kretchmer and Karveth (2001) note that the study of race in cyberspace has often lead to paradoxical inferences. For example, they point out that on the one hand, the Internet has provided both an opportunity to discover and a forum to confront racial issues; On the other hand, however, cyberspace could be viewed as providing forums that have perpetuated, or perhaps even enhanced, aspects of racism. In support of the latter point of view, the Internet has introduced new tools, techniques, and forums for harassing members of racial and ethnic groups. In this sense, Internet technology can be viewed as a vehicle that has magnified both the significance and rhetoric of some racially motivated hate groups.

Lynn Theismeyer has examined some of the "rhetorical roles" that the Internet plays with respect to race. Her analysis of the rhetoric of racism does not focus on specific racial and minority groups in the United States, such as African Americans and Hispanics, but rather on the rise of neo-Nazi propaganda internationally. Theismeyer describes two distinct kinds of racist speech that have proliferated on the Internet: (i) online communications (music, images, broadcasts, etc.) that "exhort users to act against target groups" and (ii) rhetoric that indirectly promotes or justifies violence.[21] We should note, however, that some instances of what Theismeyer describes as racially controversial "rhetoric" would likely be protected in the

United States under the First Amendment right to free speech. So, it has not been easy to control certain forms of online racist rhetoric in the United States.

As we saw in Chapter 9, some European countries, especially Germany and France, have made a greater effort than the United States to restrict online hate speech that has targeted racial groups; this has been especially apparent in the case of neo-Nazi organizations. We also saw (in Chapter 9) that the U.S. government has focused more on censoring pornography, which many also view as offensive speech, than it has on efforts to combat online hate speech affecting race. This has allowed for some White supremacist groups in the United States, including the Ku Klux Klan (KKK), to establish Web sites for organizing demonstrations and spreading their messages of racial prejudice.[22] The designers and operators of these Web sites have also sometimes used misleading and deceptive keywords to attract visitors. For example, racist Web sites have deceptively used keywords, such as "Martin Luther King Jr.," to lure unsuspecting persons to their sites. So, someone searching for information about Dr. King's life might be directed to a Web site where he or she is instead subjected to racist hate speech directed against African Americans.

To what extent have racist Web sites influenced and possibly exacerbated, racial prejudice in the United States, as well as at the international level? Theismeyer believes that, at this point, it is not yet possible to know whether online technologies have been the main cause of the rapid spread of racism, especially in the neo-Nazism movement in Europe. However, she is convinced that the Internet has been its principal tool.[23]

In Section 10.5.2, we examine some ways in which blogs and the blogosphere also can either directly or indirectly contribute to the promotion of racial prejudice online. For example, some extreme right-wing political blogs have portrayed U.S. President Barack Obama in ways that are generally considered to be offensive and demeaning to African Americans. On the one hand, these blogs include content that is protected by free speech; on the other hand, they can reinforce racial stereotypes and perpetuate racial prejudice.

► 10.4 CYBERTECHNOLOGY AND GENDER

Other equity-and-access concerns associated with cybertechnology in general, and with the digital divide in particular, can be analyzed with respect to gender. Feminist authors and others who advocate for women's issues proffer arguments similar to those advanced by or on behalf of African Americans (and other racial minorities), which we examined in the preceding section. Women, like the members of many racial and ethnic groups, have not always been included in important decisions about technology policies and, until very recently, have not participated to the same degree as men in the use of technology.

We can begin by noting that the gap that has traditionally existed between the percentage of female and male Internet users in the United States had narrowed significantly by the beginning of the twenty-first century. A report by the *Pew Internet & American Life Project* in 2005 noted that young women were slightly more likely to be online than young men and that the number of black women online surged between 2002 and 2005 (to the point where black women who used the Internet outnumbered black men by about 10%). Pew Internet Project surveys conducted in 2005 also reported that in the United States, 66% of women went online, as opposed to 68% of men. But some analysts noted that women slightly outnumbered men in the Internet-user population because women made up a greater share, that is, proportionally, of the overall U.S. population. By 2008, however, even the percentage of women who used the Internet was equal to that of men.[24]

Although the gap between female and male Internet users has narrowed considerably in many Western countries, this has not been the case globally. However, some specific global initiatives have been introduced to address problems underlying gender equity and access in

non-Western nations.[25] But even if the global divide between men and women who enjoy access to digital technology has been narrowed, we can ask whether that fact in itself is sufficient to resolve the core gender-related controversies? Adam (2005) argues that gender issues involving cybertechnology are much more complex than concerns about levels of online access. For example, we will see that gender issues also arise because of bias in software design, as well as the portrayal of women in many video games.

We next examine gender-related cybertechnology issues in terms of two important categories:

i. Women's access to high-technology jobs/careers

ii. Gender bias in software design (especially in video games)

10.4.1 Access to High-Technology Jobs

Some authors believe that to better understand gender-related issues affecting cybertechnology, we need to examine the challenges facing women who consider jobs and careers in computer science and engineering. To that end, Camp (1997) has conducted research on what she and others call "pipeline issues" by analyzing statistics involving the number of women entering the computer science and engineering professions; the data collected during the past 25 or so years suggest that proportionately few women elect to pursue degrees in either field. Wessells (1990) pointed out that in 1989, fewer than 5% of those awarded PhD degrees in computer science were women. According to slightly later statistics provided by Camp, in 1997, that number had increased to 15.4% (during 1993–1994). However, Camp also noted that the percentage of women pursuing bachelors and masters degrees in computer science had declined slightly during those years.

Kirlidog, Aykol, and Gulsecen (2009) cite more recent evidence to support the ongoing concerns about the "pipeline," and they argue that computer science is still typically regarded as a "male profession," both in industry and academia. The authors also claim that women remain in the "margins" of a male-dominated profession, which is filled with highly gendered expressions such as "killing or aborting programs," "workbench," "toolkit," etc., that reflect the masculine culture of the field. Kirlidog et al. identify three "net results" of the male-dominated computing profession in which women are:

1. Underrepresented in computer-related jobs

2. (Even more) underrepresented in the managerial ranks in the computing field because of the "glass ceiling"

3. Paid less than men for doing the same jobs[26]

To support (1), they cite a study showing that while 46% of the United States workforce was made up of women, only 28% of computer science and mathematics-related jobs were held by women. This problem is by no means unique to the United States or to Western nations, they argue, because a large discrepancy can also be found in the computing field in developing nations such as India. With regard to (2), they show how women in India and elsewhere are underrepresented not only in terms of the number of hi-tech jobs but also in the number of managerial positions in the computing field. In support of (3), the authors point out that (i) the average woman in India earns approximately 60% of what a man is paid for the same job, and (ii) only 3% of management-level jobs are held by women.[27]

So the "pipeline" concerns regarding the low numbers of women entering the computer profession (initially reported in the late 1980s and early 1990s), as well as the limited career opportunities for women who entered the profession, seem to have persisted well into the twenty-first century. Many of those who monitor the pipeline believe that we need to worry

about some implications that this continued trend could have for the future of the computing field. Some note, for example, that "pipeline statistics" provide us with projections regarding the proportion of women who will likely be able to contribute in critical areas of the computer/IT professions such as those affecting national security. For example, Spafford (2014) worries that more women are already needed, and will likely continue to be needed, in the field of cybersecurity.

Before concluding this section, we should note that some authors writing on the topic of gender and computing have been critical of approaches that focus solely, or even mainly, on access-related or "pipeline" issues. For example, Adam (2004, 2005) notes that while examining the low numbers of women in the computing profession is important because it reveals existing inequities in the field, this approach also tends to severely limit the study of gender and computing issues mainly to access-related concerns. Adam also believes that focusing on this approach may cause us to miss an opportunity to use feminist ethical theory in our analysis of broader cyberethics issues such as privacy and power in terms of their gender implications. She worries that current computer ethics research involving gender is "undertheorized," and she argues that we need a "gender-informed ethics" to improve the process. For example, Adam argues that this theory helps us to better understand issues such as cyberstalking and Internet pornography in ways that traditional ethical theories cannot.[28] Unfortunately, however, a fuller examination of Adam's gender-informed ethical theory is beyond the scope of this chapter.

10.4.2 Gender Bias in Software Design and Video Games

Some authors have argued that in the past, educational software tended to favor male learning behaviors and thus was biased against female learners. So, there was some concern then about the effect that gender bias in educational software programs might have for young female students. Although concerns about this kind of gender bias have dissipated in recent years, critics argue that gender bias can still be found in many other kinds of software applications. This is especially apparent in the case of video game software.

Buchanan (2000) argues that bias in the development of video games has raised two distinct kinds of ethical concerns because these games tend to:

1. Either misrepresent or exclude female characters
2. Perpetuate traditional sexist stereotypes

With respect to (1), she argues that the representational politics of gender in video games needs greater evaluation, because many computer games, especially virtual sports games, include no female characters at all. And with regard to (2), Buchanan argues that some video games, such as Barbie Fashion Designer, have reinforced traditional cultural stereotypes along gender lines.

Some might tend to dismiss concerns about gender bias in video games on the grounds that many women simply aren't interested in them. However, Brey (2008) argues that the question of gender bias in these games is nevertheless "morally significant." He points out, for example, that if:

> computer games tend to be designed and marketed for men, then women are at an unfair advantage, as they consequently have less opportunity to enjoy computer games and their possible benefits. Among such benefits may be greater computer literacy, an important quality in today's market place.[29]

Brey also notes that many analysts believe that the computer industry is mainly to blame for the gender gap that exists in the video game industry. For example, most game developers are male; also, there has been little interest on the part of developers to design suitable games for women. Additionally, Brey points out that very few computer games include decent role

models for women. He also notes that a disproportionate number of the female characters in these games are strippers or prostitutes and that these characters tend to have "unrealistic body images." (Brey's points are further examined in Chapter 11 in our discussion of ethical aspects of virtual environments and virtual reality applications, including video games.) We conclude this section by noting that Brey and Buchanan each make a plausible case for how the design of video games contributes to gender bias and for why that bias is indeed morally significant.

▶ 10.5 CYBERTECHNOLOGY, DEMOCRACY, AND DEMOCRATIC IDEALS

In previous sections of this chapter, we examined equity-and-access issues pertaining to social/economic class (the digital divide), race, gender, and disabled persons. Underlying many of the concerns involving these diverse sociodemographic groups were issues that also affect democracy, in particular, as well as democratic ideals and values in general. Not surprisingly, then, a number of interesting questions arise at the intersection of democracy and cybertechnology. For example, some authors question whether the Internet is an inherently democratic technology, while others question whether we should develop the Internet along democratic principles.[30] In our analysis of democracy and cybertechnology, however, we consider two slightly different kinds of questions:

1. Has the use of cybertechnology (so far) enhanced democracy and democratic ideals or has it threatened them?
2. What impact has the use of cybertechnology had on the political election process in democratic nations?

10.5.1 Has Cybertechnology Enhanced or Threatened Democracy?

Why should we care whether cybertechnology favors and possibly enhances democracy, or whether it instead threatens and potentially undermines it? We can begin by noting that democracy, when compared to alternative forms of government, seems an attractive political structure and, arguably, one of the fairest. Because of these assumptions, Graham (1999) points out that it is difficult to get people, especially in the Western world, to engage in a serious debate about the merits of democracy. He correctly notes that democracy, along with its corresponding notion of a "democratic ideal," has won almost universal and largely unquestioning acceptance in the West. Graham also points out, however, that not all political theorists and philosophers have regarded democracy as the best—or, in some cases, not even as an adequate—form of government. For example, he notes that in *The Republic*, Plato was highly critical of democracy and viewed it as a form of mob rule in which important decisions could be made by a citizenry that typically was not well informed on matters involving the state. And Graham also notes that in the nineteenth century, philosopher John Stuart Mill questioned whether democracy was indeed the ideal form of government.[31]

Let us assume, for the sake of argument, that democracy is superior to alternative political structures. We can still ask whether cybertechnology favors democracy and democratic ideals. Many who believe that it does tend to point to one or more of four factors, that is, where the Internet is alleged to provide greater:

- **a.** *Openness* (i.e., an open architecture)
- **b.** Empowerment
- **c.** Choice
- **d.** Access to information

With regard to (a), some authors argue that the Internet provides an open forum in which ideas can generally be communicated freely and easily. Other authors, focusing on (b), note that the Internet empowers certain groups by giving them a "voice," or say, in some matters that they had not previously had. Still other authors, such as Graham, suggest that the Internet empowers individuals by giving them more choices and thus greater freedom.[32] And Sunstein (2001, 2007) points out that the Internet has provided greater access to information at a lower cost. Perhaps Introna and Nissenbaum (2000) sum up these points best when they note that in the early days of the Internet, people tended to assume that online search technologies would:

> give voice to diverse social, economic, and cultural groups, to members of society not frequently heard in the public sphere [and] empower the traditionally disempowered.[33]

Values affecting openness, empowerment, choice, and greater access to information all seem to favor democracy. Thus, insofar as cybertechnology facilitates these values, it would also seem to favor democracy and democratic ideals. But does the Internet's "open" architecture necessarily facilitate democratic values universally? Consider that some countries have gone to great lengths to censor political speech in cyberspace. For example, China required Google to comply with strict rules for filtering information, which many nations in the West would view as unacceptable. Also, Saudi Arabia has censored political speech online. So, nondemocratic countries have found some ways around the "open" architecture of the Internet and its ability to spread information freely.

Graham worries that some features of the Internet may even contribute to the "worst aspects" of democracy by fostering social and political fragmentation. A similar kind of concern is raised by Diaz (2008) when he asks whether Internet search technologies will filter out, and thus exclude, the kinds of "independent voices and diverse viewpoints" that are essential for a democracy. This worry is echoed by Pariser (2011) who believes that democracy is now threatened by a new mode of filtering on the Internet, involving "personalization filters," which are currently used by major search engines. We briefly consider each type of threat.

Social/Political Fragmentation and "Personalization" Filters

How does the Internet facilitate social and political fragmentation, and why is fragmentation problematic for a democratic society? The Internet fragments society by facilitating the formation of groups who depart from the mainstream perspectives of a cohesive society. An analogy involving television news programming in physical space might help us appreciate how easily social and political fragmentation can occur and why it can be problematic. Consider that until the advent of cable TV news programming in the 1970s, American television viewers relied primarily on the three major networks for the evening news reports. Even though the program formats varied slightly and even though different anchors delivered the news to viewers, all three presented "mainstream" news reporting that satisfied certain standards of accuracy and credibility before the networks would broadcast it. At times, the members of political groups may have been annoyed with, or possibly even offended by, the way that a particular story was presented, but the news reports were generally descriptive or factual. Some news programs also included commentaries, usually toward the end of the program, in which the commentator expressed an opinion, but there was a clear line between "factual" reporting and personal opinion.

Now you can select a news program that fits best with and reinforces your political ideology. For example, consider a news report of hostilities between Israelis and Palestinians. If supporters of Israel do not like the way the story is reported on an American news network, and if they have cable or satellite access to Israeli television, they can tune into an Israeli station for their news. Similarly, if Palestinian supporters dislike the American media's coverage, and if they have cable access to an Arab news network such as Al-Jazeera, they can choose to view the news story as broadcast via an Arab television station. On the one hand, these options provide

supporters of both sides in this conflict with greater choices and seemingly greater freedom. On the other hand, these options can also increase social and political fragmentation.

We can apply a similar analogy to news reports of domestic political issues in the United States. Conservatives and liberals can each interact in online forums and visit Web sites that exclusively promote the political views that they embrace. Of course, a critic could point out that prior to the Internet, many people subscribed to newspapers and magazines that were labeled as either radically liberal or radically conservative and therefore biased in their reporting. But it is more difficult to filter information in physical space because people in most physical communities encounter individuals with ideological perspectives different from their own, even when they seek out only those who share their belief systems. In online forums, however, it is possible for individuals to be in contact with only those people who share their ideological beliefs. Thus, Epstein (2000) worries that in the near future, the concept of the "public square," where ideas have been traditionally debated could become *fragmented* into "thousands of highly specialized communities that do not communicate with one another."

Internet Filtering, Polarization, and Deliberative Democracy

As noted above, some critics now also worry about the impact that "personalization filters" used by contemporary search engine companies will have for democratic societies. Pariser fears that these filters enable a kind of "invisible autopropaganda," which can indoctrinate us with our own ideas. He notes that while democracy "requires citizens to see things from one another's point of view," we are instead increasingly "more enclosed in our own bubbles." He also notes that while a democracy "requires a reliance on shared facts," we are instead being presented with "parallel but separate universes."

Why is this trend away from citizens having shared facts so dangerous for a democracy? For one thing, consider the contentious debate about climate change in the United States during the past decade. Pariser points out that studies have shown that between 2001 and 2010, the views of people's beliefs about whether the climate was warming changed significantly along Republican vs. Democrat lines. The number of Republicans who believed that the planet was warming fell from 49% to 29%, while the number of Democrats rose from 60% to 70%. How is such a discrepancy regarding beliefs about climate change possible among people living in the same country? Pariser notes that a user's online search for "climate change" will turn up different results for an environmental activist than for an oil company executive; it will also generate different results for users whom the search algorithm understands to be Democrats rather than Republicans.

With entrenched views about current controversial topics such as climate change, citizens in democratic countries such as the United States are becoming increasingly polarized. Cass Sunstein worries that increased polarization threatens *deliberative democracy*—that is, the process of rationally debating issues in a public forum. He suggests that deliberative democracy may suffer irreparable harm because of the ways in which the Internet now filters information.

Why does Sunstein believe that deliberative democracy is threatened by Internet filtering? For one thing, he worries that people using software filters will not be inclined to gather new information that might broaden their views but will instead use information available to them on the Internet to reinforce their existing prejudices. Sunstein's concerns are echoed by Diaz (2008), who points out that if we wish to preserve the principles of deliberative democracy, we need to make sure that a "broad spectrum of information on any given topic" is disseminated on the Internet. A similar point is also made by Hinman (2005) when he argues that "free and undistorted access to information" is essential for a deliberative democracy to flourish. So, if these critics are correct, there are good reasons to be skeptical that cybertechnology, in the near term at least, will facilitate values essential for deliberative democracy.

We can conclude this section by noting that, as Sunstein suggests, cybertechnology seems to have both democracy-enhancing and democracy-threatening aspects. We saw that the

Internet's open architecture, which enables greater access to information and for that information to be shared freely and easily, would seem to enhance some democratic values. However, we also saw how Internet filtering schemes enable fragmentation and polarization that, in turn, undermine deliberative democracy.

10.5.2 How has Cybertechnology Affected Political Elections in Democratic Nations?

We now turn to our second principal question regarding democracy and cybertechnology: How has this technology impacted political elections so far? In answering this question, we look at the impact via two broad categories: (i) using electronic devices and social media sites for political fundraising, influencing voter turnout, and organizing political demonstrations and (ii) using political blogs to spread false information that could influence election outcomes. We begin with (i).

Electronic Devices and Social Media

Graham suggests that in representative democracies, such as the United States, cybertechnology might be used to concentrate more power in the hands of elected representatives instead of ordinary citizens. He also notes that many representatives and political leaders (including their staffs) tend to have both greater technological resources and the ability to use them more skillfully than many ordinary citizens. These factors, in Graham's view, suggest that those in power can effectively use these technological resources to retain their power. We can ask whether the following example illustrates Graham's point. In the 2004 U.S. presidential elections, Carl Rove, a former advisor in the George W. Bush administration, used BlackBerry (smartphone) technology to coordinate with Republican officials across all of the voting precincts in Ohio, a "battleground state" that would determine the winner of that year's election. Some political commentators suggested that Roves coordinating a state-wide, get-out-the-vote effort to target voters via the use of BlackBerry technology helped to ensure victory in Ohio, which provided the necessary electoral votes for President Bush to remain in power for four more years. Although it is difficult to prove that Rove's use of this technology helped the incumbent president to remain in power in 2004, we can see how the use of the latest technology in a state or national election can influence the voter turnout and ultimately the outcome of that election.

Next, consider that as Barack Obama prepared to run in the 2008 U.S. presidential elections, his staff organized a "grassroots" fund-raising strategy on the Internet through various social networking sites (SNSs) to raise millions of dollars (mostly as small contributions from young people) to finance his presidential campaign. (We examine SNSs in detail in Chapter 11.) In running for his second term in 2012, however, it was not clear whether his staff's use of the latest social media technologies helped him to win reelection and remain in power for four additional years. Yet, it would seem that Graham's claim may still have some merit. For example, we have seen how some political parties in power (in Western democracies, at least) have successfully used the latest available cybertechnologies to maintain their power. On the other hand, however, ordinary citizens in some nondemocratic countries, such as Tunisia and Egypt, have used electronic devices and social media to topple the powerful political regimes in those nations.

Recall our brief analysis of the "Arab Spring" in Scenario 10-1. There, we saw how a political movement that began in early 2011 in the Arab world succeeded in bringing down a series of governments largely because ordinary citizens had used digital technologies such as electronic devices and social media to organize their protests. So, it would seem that Graham's claim about political leaders in representative democracies being able to use technology to remain in power would not necessarily apply in the case political leaders in some nondemocratic nations.

Political Blogs and the Democratic Process

We next consider the impact that blogs (or Weblogs), especially political blogs, can have on democracy. (We discuss some broader ethical and social impacts of blogs and the "blogosphere" in more detail in Chapter 11 in connection with our analysis of online communities.) To what extent do political blogs reinforce democratic values and ideals, and how can they undermine them? Insofar as blogs function as instruments for communicating and disseminating information about important political issues, they would seem to reinforce values that favor democracy. But the standards for ensuring accuracy of the content posted in political blogs are not always adequate.

During the 2008 U.S. presidential elections, some extreme right-wing political bloggers reported that (then presidential candidate) Barack Obama was a Muslim and that he was not born in the United States.[34] At the same time, some radical left-wing bloggers reported that (vice presidential candidate) Sara Palin's youngest child was really her grandchild and that Palin was protecting her unmarried daughter from embarrassment.[35] Neither story was vetted in the way that a report submitted by a professional journalist working for a reputable news organization would be, and neither story would likely have been published in a reputable newspaper. But these stories were read online by numerous people, many of whom may have assumed the reports about Obama and Palin to be true merely because they were published on the Internet.

As (hard copy) newspaper subscriptions continue to decline, and as more and more people get their news online, we may have to worry about the standards of accuracy that apply in the online political news media, especially political blogs. As we noted above, a democracy depends on the dissemination of truthful information to flourish and survive. So perhaps we should be concerned about the lack of veracity in some political blogs and the implications that the mass dissemination of false information online may have for the future of democracy.

However, some analysts do not seem concerned about the potentially negative effects of blogging for democracy. For example, Goldman (2008) points out that even if individual blogs are biased, it doesn't follow that the entire blogosphere is. (Recall our discussion of the Fallacy of Composition in Chapter 3, where we saw that attributes that apply to the part do not necessarily apply to the whole.) As Goldman aptly puts the matter, "the reliability of the blogosphere shouldn't be identified with the reliability of a single blog."[36] Goldman also believes that it is possible that the blogosphere may ultimately contribute to the preservation of democratic values.

In concluding this section, we note that many controversial issues affecting cybertechnology and democracy have not been examined. For example, there are controversies surrounding e-voting, as well as the selling of votes online; unfortunately, these and other issues are beyond the intended scope of this chapter. Note also that our brief analysis of some key cybertechnology and democracy issues in Section 10.5 was not intended to be exhaustive.

► 10.6 THE TRANSFORMATION AND THE QUALITY OF WORK

In Sections 10.1–10.5, we examined questions pertaining to equity-and-access issues as they affect both *sociodemographic groups*—for example, disabled persons, racial minorities, and women—and *social/political institutions*, mainly as they impact democracy and democratic values. In this section, we consider some equity-and-access-related issues from a third perspective or social category. Here, we examine the impact of cybertechnology on a *social sector*: the contemporary workplace. Though still relatively new, cybertechnology already has had a profound effect on employment as well as on the nature of work itself. Computers and cybertechnology also significantly affect the quality of work life. Before considering this impact, however, we examine issues involving the transformation of the contemporary workplace and the displacement of jobs.

10.6.1 Job Displacement and the Transformed Workplace

While it is debatable whether cybertechnology has benefited workers, overall, it is quite clear that this technology has significantly changed the workplace. Some have gone so far as to suggest that cybertechnology has *transformed* the nature of work itself. One question that frequently arises in discussions about the transformation of employment by cybertechnology is whether, on balance, it has created or eliminated more jobs. There are arguments to support both sides of this debate. Although cybertechnology has caused certain industries to eliminate human jobs, it has enabled other industries, such as computer support companies, to create jobs; social scientists often refer to this shift as *job displacement*. We examine some key issues involving job displacement from two broad perspectives or categories:

A. Automation, robotics, and expert systems

B. Remote work, outsourcing, and globalization

Whereas job displacement issues affecting (A) typically result from the introduction of new kinds of machines (hardware) as well as new software applications, those affecting (B) often result from changes in policies and practices involving employment and the workplace (that, in turn, are often influenced by technological developments). We begin with a brief analysis of (A).

Automation, Robotics, and Expert Systems

Job displacement is often associated with *automation*. Social and ethical issues involving automation are by no means new, nor are they unique to cybertechnology. Social scientists note that the Industrial Revolution transformed jobs into smaller, discrete tasks that could be automated by machines, creating working conditions that adversely affected the lives of many workers. When new automated technology threatened to replace many workers, one group of disenchanted workers in England—later referred to as "Luddites"—smashed machines used to make textiles. ("Luddite" is derived from a nineteenth-century British worker, Ned Ludd, who reputedly led workers in destroying factory machinery.)

Just as the Luddites resisted factory technology in the nineteenth century because they thought it threatened their jobs and thus their livelihoods, some workers have opposed developments involving cybertechnology for similar reasons. In the 1970s, for example, workers tried to stall developments in microprocessor-based technology, fearing that it would lead to a loss of jobs. Workers as well individuals in general who resist technological change, and who have a pessimistic view of the impact of cybertechnology in the workplace, are sometimes referred to as neo-Luddites.

Developments in *robotics* have also raised social concerns affecting job displacement. Robots, equipped with motor abilities that enable them to manipulate objects, can be programmed to perform tasks that are either (i) routine and mundane for humans or (ii) considered hazardous to humans. As Lin (2012) so aptly puts it, robots are typically tasked to perform the "three Ds"—that is, jobs that humans consider "dull, dirty, and dangerous." Although robots were once fairly unsophisticated, contemporary robotic systems are able to perform a wide range of tasks. (We examine some ethical aspects of robots and robotic systems in detail in Chapter 12.)

Whereas (physical) robots have eliminated many blue-collar jobs, sophisticated programs called expert systems (*ESs*) threaten many professional jobs. An ES is a problem-solving computer program that is "expert" at performing one particular task. ESs use "inference engines" to capture the decision-making strategies of experts (usually professionals); they execute instructions that correspond to a set of rules an expert would use in performing a professional task. A "knowledge engineer" asks human experts in a given field a series of questions and then extracts rules and designs a program based on the responses to those questions. Initially,

ESs were designed to perform jobs in chemical engineering and geology, both of which required the professional expertise of highly educated persons and were generally considered too hazardous for humans. More recently, ESs have been developed for use in professional fields such as law, education, and finance.

The use of ESs, much like the use of (physical) robotic systems, has raised some ethical and social issues having to do with "de-skilling" and "worker alienation." We noted the impact that automation had on some workers during the Industrial Revolution. Social scientists have suggested that prior to that period, workers generally felt connected to their labor and exhibited a strong sense of pride and craftsmanship. The relationship between worker and work began to change, however, when work became automated. Social scientists have used the term *alienation* to describe the effect that de-skilling had for workers whose skills were transferred to machines. Mason (2007) cites as an example the introduction of Jacquard's loom and its effect on weavers during the Industrial Revolution, where skills were "disembodied" from weavers and craftsmen and then "reembodied" into machines such as the loom.

Today, ES technologies pose a similar threat to professional workers by allowing knowledge, in the form of rules applying to knowledge-related skills, to be extracted from (human) experts and then embedded into computer software code. Mason points out that knowledge can now be "disemminded" from professional workers, or experts in a given field, and "emminded" into machines in the form of computer programs. Mason also believes that there is an interesting connection between the Industrial Revolution and the current era in that a proliferation of publications on ethics appears in each time period, and he suggests that working conditions during the Industrial Revolution may have been responsible for the greatest outpouring of moral philosophy since Plato and Aristotle. He notes, for example, that works on ethics by Immanuel Kant, Jeremy Bentham, and John Stuart Mill appeared during that era. Mason also suggests that, similarly, contemporary workplace controversies associated with cybertechnology have contributed to the recent flurry of publications on ethics.[37]

We conclude this section by noting that automation, robotics, and ESs have each contributed significantly to job displacement in the contemporary workplace. We have also noted that these three technologies have adversely affected some employee groups more than others. Next, we examine the impact that three relatively recent employment-related practices and policies have had for job displacement, in particular, and the contemporary workplace in general.

Remote Work, Job Outsourcing, and Globalization

One factor that has transformed work for many employees is that cybertechnology has made it possible for them to work "remotely"—that is, outside the traditional workplace. Even though remote work, referred to by some as "telework," is a relatively recent practice, it has already raised social and ethical questions. One question has to do with whether all employees who perform remote work benefit from it equally. For example, are white-collar employees affected in the same way as employees who are less educated and less skilled? It is one thing to be a white-collar professional with an option to work at home at your discretion and convenience, but it is very different for some clerical, or "pink collar," workers who may be required to work remotely out of their homes. Of course, some professional men and women may choose to work at home because of childcare considerations or because they wish to avoid a long and tedious daily commute, but employers may require other employees, especially those in lower skilled and clerical jobs, to work at home. In some case, people required to work remotely may not have the same opportunities for promotions and advancements as their (more visible) counterparts who have the option of working in a traditional workplace setting. So, employees in some situations may be disadvantaged because of specific remote work policies.

Another contemporary practice contributing to the ongoing transformation of work involves job *outsourcing*. Outsourcing practices have affected the displacement of jobs not

only for employees in industries within countries but also across them, and thus have had international implications. Until recently, most American jobs affected by remote work still remained in the United States. Now, many jobs are outsourced to countries where labor costs are less expensive. For example, many traditional manufacturing jobs in the United States have been exported "offshore." Initially, this phenomenon impacted mainly traditional "blue-collar" jobs; now it also affects many jobs in the service sector. In the past decade or so, it has also affected many highly skilled "white-collar" jobs such as those in the computing/IT field. Consider, for instance, that many programming jobs traditionally held by employees in American companies are now "outsourced" to companies in India and China whose employees are willing to work for significantly lower wages than those paid to American programmers. Ironically, perhaps, the jobs of the programmers who had the high-tech skills needed to make possible the outsourcing of many white-collar jobs are now being outsourced to countries where programmers earn less money.

Controversies affecting job outsourcing, especially where multiple nations are involved, are often linked to a phenomenon that has come to be known as *globalization*. What is globalization, and how is it affected by cybertechnology? Monahan (2005) defines globalization as "the blurring of boundaries previously held as stable and fixed . . . between local/global, public/private [and] nation/world."[38] Monahan notes that discussions of globalization tend to focus on concerns involving labor outsourcing, international trade agreements, immigration concerns, cultural homogenization, and so forth. So there are broad cultural issues, as well as economic controversies, underlying the debate about globalization. In this section, however, our concern is with the economic aspects of globalization, particularly as they impact cybertechnology and the workplace.

In a global economy where individual nations are protected less and less by tariffs, competition between countries for producing and exporting goods, as well as for providing services, has escalated. In the United States, considerable debate has focused on the North American Free Trade Agreement (NAFTA) initiatives during the past two decades. Those individuals and organizations that have been labeled "isolationists" and "protectionists" have opposed NAFTA, while proponents of "open" markets between countries have tended to support it. Do trade agreements such as NAFTA and General Agreement on Tariffs and Trade (GATT) favor poorer countries that are part of the agreement where the cost of labor is cheaper? Or, do these trade agreements favor the majority of people in wealthier countries who are able to purchase more goods and services at lower prices? On the one hand, NAFTA and GATT have encouraged greater competition between nations and, arguably, have resulted in greater efficiency for businesses. On the other hand, the economies of some nations have been severely impacted by the job loss that has resulted.

What is the net economic benefit of globalization for both the richer and the poorer countries? To what extent has cybertechnology exacerbated the concerns raised by globalization and the displacement of jobs? These questions are controversial, and proponents on each side have come up with drastically different statistical data to support their claims. However, it is quite apparent that both globalization and job outsourcing have had a significant impact on the "quality of worklife" of numerous employees—a technology-and-work-related issue that we examine in the following section.

10.6.2 The Quality of Work Life in the Digital Era

So far, we have focused on social and ethical issues surrounding the transformation of work vis-à-vis job displacement, but many social scientists have also questioned how cybertechnology impacts the *quality* of work life. Quality issues include concerns about employee health, which can pertain both to physical and mental health-related issues. Among these concerns are worries about the level of stress for many employees in the contemporary workplace, especially those who are subject to computerized monitoring and surveillance.

Employee Stress, Workplace Surveillance, and Computerized Monitoring

Many workers experience stress because their activities are now monitored closely by an "invisible supervisor"—that is, by cybertechnology, which can record information about one's work habits. The *2007 Electronic Monitoring and Surveillance Report*, sponsored by the American Management Association (AMA) and published by the AMA/ePolicy Institute Research (2008), noted that 43% of American companies monitor employee e-mail, and 96% of those companies "track external (incoming and outgoing messages)." The report also noted that 45% of companies track the amount of time employees spend on their company-owned devices. An increasing number of these companies now also monitor the blogosphere (described in Chapter 11) to see what is being written about them in various blogs, and some also monitor SNSs such as Facebook. As a result of increased monitoring, many employees have been fired for misusing a company's e-mail resources or its Web resources, or both. So, the threats posed by computerized monitoring would clearly seem to contribute to employee stress.

Perhaps somewhat ironically, data entry clerks and so-called "information workers," whose work is dependent on the use of computer technology to process information, are among the groups of employees who have been most subjected to monitoring by that technology. Although computer monitoring techniques were initially used to track the activities of clerical workers such as data entry operators, they now also track and evaluate the performance of professionals, such as programmers, loan officers, investment brokers, and managers. And nurses are also frequently monitored to make sure that they do not spend too much time with one patient.

Why is employee monitoring via computerized surveillance tools increasing so dramatically? Kizza and Ssanyu (2005) identify multiple factors that have contributed to the recent expansion and growth of employee monitoring, two of which are worth highlighting for our purposes: (i) cost (the lower prices of both software and hardware) and (ii) size (the miniaturization of monitoring products). The lower cost of monitoring tools has made them available to many employers who, in the past, might not have been able to afford them. And the miniaturization of these tools has made it far easier to conceal them from employees.

Introna (2004) points out that surveillance technology, in addition to becoming less expensive, has also become "less overt and more diffused." He also believes that current monitoring technologies have created the potential to build surveillance features into the "very fabric of organizational processes." Consider that monitoring tools are used to measure things such as the number of minutes an employee spends on the telephone completing a transaction (e.g., selling a product or booking a reservation) and the number and length of breaks he or she takes. Monitoring software can even measure the number of computer keystrokes a worker enters per minute. Weckert (2005) notes that an employee's keystrokes can be monitored for accuracy as well as for speed and that the contents of an employee's computer screen can easily be viewed on the screen of a supervisor's computer (without that employee's knowledge).

Employees using networked and mobile electronic devices can also be monitored outside the traditional workplace. For example, some employees work at home on employer-owned devices or via an employer's networked application, and some use employer-owned electronic devices to communicate with fellow workers and customers while they are traveling. Consider the following scenario involving a city employee's use of a pager (device).

▶ **SCENARIO 10–3:** Employee Monitoring and the Case of *Ontario vs. Quon*

Jeff Quon, a police officer, was an employee of the city of Ontario, CA. City employees in Ontario agreed to a policy in which the city reserved the right to monitor ("with or without notice") their electronic communications, including Internet use and e-mail. In 2001, 20 police officers in the SWAT Unit of the

Ontario Police Department (OPD) were given alphanumeric pagers. Quon was one of the officers who received a pager. The police officers were told that they were allowed a fixed limit of 25,000 characters per month on their pagers, in accordance with the terms of a contract that OPD had with the Arch Wireless (now USA Mobility) service provider. The officers were also told that if they exceeded that monthly limit, they would be charged a fee for overuse. Quon exceeded the limit on his pager for two consecutive months, and he paid the city for the excess usage. However, his pager was subsequently audited by OPD, which requested a transcript of his messages from Arch Wireless.

During the audit, it was discovered that many of Quon's messages were personal (and thus not work related) and that some were sexually explicit. Quon was then disciplined for violating the city's electronic communications policy. But Quon challenged OPD and the city of Ontario, arguing that his privacy rights had been violated; he alleged that the audit of the content on his pager was both a violation of his constitutional privacy right (under the Fourth Amendment), as well as a violation of federal telecommunications privacy laws. Quon also argued that the city's employee monitoring policy did not explicitly mention pagers and text messages, and he noted that the officers who received pagers were told verbally that they could use their pagers for "light personal communications." However, OPD pointed out that the officers were also informed that obscene, defamatory, and harassing messages on the pagers would not be "tolerated."

The Ninth Circuit Court in California initially sided with Quon (and the other officers involved in the suit). However, the case was eventually appealed to the U.S. Supreme Court, which ruled (in June 2010) that the audit of Quon's pager was work related and that it did not violate Quon's Fourth Amendment rights involving unreasonable search and seizure.[39] ■

Did the Supreme Court make the correct decision in this case? Or, did Quon have a reasonable expectation of privacy in this particular incident, as the lower court initially ruled? Should there be any limitations or constraints placed on an employer's right to monitor an employee's conversations on electronic devices? Or, should all forms of employee monitoring be permissible, where employer-owned equipment is involved? The case involving Jeff Quon may cause us to consider whether some additional, and perhaps more explicit, distinctions need to be drawn in the context of employee monitoring.

Distinguishing between Two Different Aspects of Employee Monitoring

Weckert (2005) argues that it is crucial to draw some distinctions involving two areas of computerized monitoring: (i) the different applications of monitoring and (ii) the different kinds of work situations (that are monitored).

Regarding (i), Weckert notes that employees could be monitored with respect to the following kinds of activities:

- e-mail usage
- URLs visited while Web surfing
- Quality of their work
- Speed of their work
- Work practices (health and safety)
- Employee interaction[40]

He points out that the reasons given to justify the application of monitoring in activities involving employee e-mail and Internet use may be very different from the kinds of justifications needed to monitor an employee's speed of work or the quality of his or her work.

With regard to (ii), some further distinctions also need to be made concerning which kinds of workers should be monitored. Weckert notes that while it may be appropriate to monitor the keystrokes of data entry workers to measure their performance in specific periods of time, it may not be appropriate to monitor the e-mail of workers in cases where client confidentially is expected. For example, he points out that a therapist employed in a health organization may

receive highly sensitive and personal e-mail from one of her client's regarding the client's mental state or physical health.

Similarly, a teacher may receive e-mail from a student, or from an academic administrator communicating about a student, that contains sensitive information regarding the student. As a college professor, for example, I occasionally receive e-mail messages from students who may disclose to me, in confidence, personal details of their health or financial status or an e-mail requesting information about a grade received for an exam or a paper. Arguably, these kinds of e-mails deserve more protection from monitoring than e-mails sent by other employees at my college who do not interact with students in ways that involve the communication of personal information that is either sensitive or confidential, or both. So, if my university were to institute an e-mail monitoring policy for its employees, factors such as these should be taken into consideration.

It is very useful to differentiate monitoring issues affecting an employee's activities in the workplace vs. issues pertaining to the kinds of workers who should or should not be monitored. These kinds of distinctions could better inform a company's policies for employee monitoring as well as the rationale(s) used to justify those policies.

Some Rationales Used to Support and to Oppose Workplace Monitoring

As in the case of many controversies involving the use of cybertechnology, employee monitoring demonstrates a clash of legitimate interests and rights for the parties involved. While employees are concerned about protecting their rights to privacy and autonomy, employers want to protect their interests involving profit margin and overall efficiency. Forester and Morrison (1994) describe some classic arguments used in favor of, and in opposition to, computer monitoring. They note that some employers defend computer monitoring on the grounds that it saves money, is essential for improving worker productivity, and helps businesses to reduce industrial espionage and employee theft.

Opponents of monitoring have a very different perspective: Some see computer monitoring as a Big Brother tactic or as an "electronic whip" used unfairly by management, and they believe it creates a work environment tantamount to an "electronic sweatshop." Some also believe that managers are motivated to use monitoring because they distrust their employees. Others claim that monitoring invades individual privacy, and thus disregards human rights. Along these lines, Rooksby and Cica (2005) argue that monitoring also poses a threat to an individual's right to "psychological autonomy."

Some critics also charge that while monitoring may accurately measure the quantity of work an employee produces, it often fails to measure the overall quality of that work. Others argue that computer monitoring is ultimately counterproductive because of its effects on employee morale. Table 10-1 lists some typical rationales used on both sides of the debate.

In concluding our discussion of employee monitoring, we should note that there are additional aspects of this controversy that we have not considered in this chapter. For example, there are now many global and international dimensions to workplace monitoring, which raise controversial questions. Coleman (2005) points out that in the global workforce, a person's

TABLE 10-1 Rationales Used to Support and to Oppose Employee Monitoring

Rationales Used to Support Monitoring	Rationales Used to Oppose Monitoring
Improves worker productivity	Increases employee stress
Improves corporate profits	Invades employee privacy
Guards against industrial espionage	Reduces employee autonomy
Reduces employee theft	Undermines employee trust

privacy could be violated by software monitoring programs that reside on a computer located in a country different from where that individual is working. This raises concerns about whether international agreements for employee monitoring policies may be needed. In fact, Coleman suggests that an International Bill of Human Rights be adopted in response to concerns affecting the global dimension of employee monitoring. Unfortunately, an examination of this aspect of monitoring, as well as Coleman's proposed solution, is beyond the scope of this chapter.

▶ 10.7 CHAPTER SUMMARY

In this chapter, we examined a wide range of equity-and-access issues affecting three broad social categories: sociodemographic groups, social and political institutions, and social sectors. With regard to demographic groups affecting socioeconomic class, we considered some implications of the digital divide at both the global and the local levels. We then examined equity-and-access issues for three additional demographic groups: disabled persons, racial minorities, and women. Next, we examined the impact of cybertechnology for one of our social/political institutions in our analysis of democracy and democratic values. Finally, we considered the impact that cybertechnology has had so far for the contemporary workplace—an important social sector. Here, we examined some equity-and-access issues as they apply both to the transformation of work (and job displacement) and to the quality of work in the digital era. Regarding the latter concern, we examined some specific challenges posed by computerized monitoring and workplace surveillance.

▶ REVIEW QUESTIONS

1. What is the "digital divide," and why is it significant?
2. What are the differences between the global digital divide and the divisions within nations affecting access to cybertechnology?
3. Are all "divides" or divisions regarding resources to goods and services ethical problems? Is the digital divide an ethical issue? Explain.
4. According to Jeroen van den Hoven and Emma Rooksby, what is meant by "distributive justice" in the context of contemporary information societies?
5. What does John Rawls mean by "primary social goods"? Can that category be extended to include "information goods," as van den Hoven and Rooksby suggest? Explain.
6. Describe three ways that Jeremy Moss believes people in developing countries are disadvantaged by lack of access to digital technology.
7. Do we have a moral obligation to bridge the digital divide? Which kinds of arguments do Maria Bottis and Kenneth Himma put forth to show why affluent countries have an obligation to bridge this divide?
8. What is the Web Accessibility Initiative (WAI), and which kinds of special equity-and-access issues affecting disabled persons has WAI addressed?
9. Describe the two perspectives from which we analyzed issues involving race and cybertechnology.
10. Describe the two main perspectives from which we viewed issues involving gender and cybertechnology.
11. Describe four ways in which the Internet can be viewed as favoring democracy and democratic ideals.
12. What is meant by "deliberative democracy"? Why does Cass Sunstein believe that Internet filters and increased polarization threaten deliberative democracy?
13. According to Gordon Graham, how does the Internet contribute to political and social fragmentation?
14. What does Eli Pariser mean by "personalization filters," and why does he believe they pose a threat for democracy?
15. What implications do political blogs have for democracy, especially for influencing the outcome of political elections in democratic nations?
16. How has work been "transformed" in the information age with respect to job displacement?
17. What are some of the ethical and social issues associated with the development and use of robots and expert systems?
18. What is globalization, and how is it related to the job outsourcing of jobs in the new global economy?
19. What is employee monitoring, and why is it controversial from an ethical perspective?
20. Describe the key arguments that have been used to defend and to oppose the use of computers and digital technology to monitor employees.