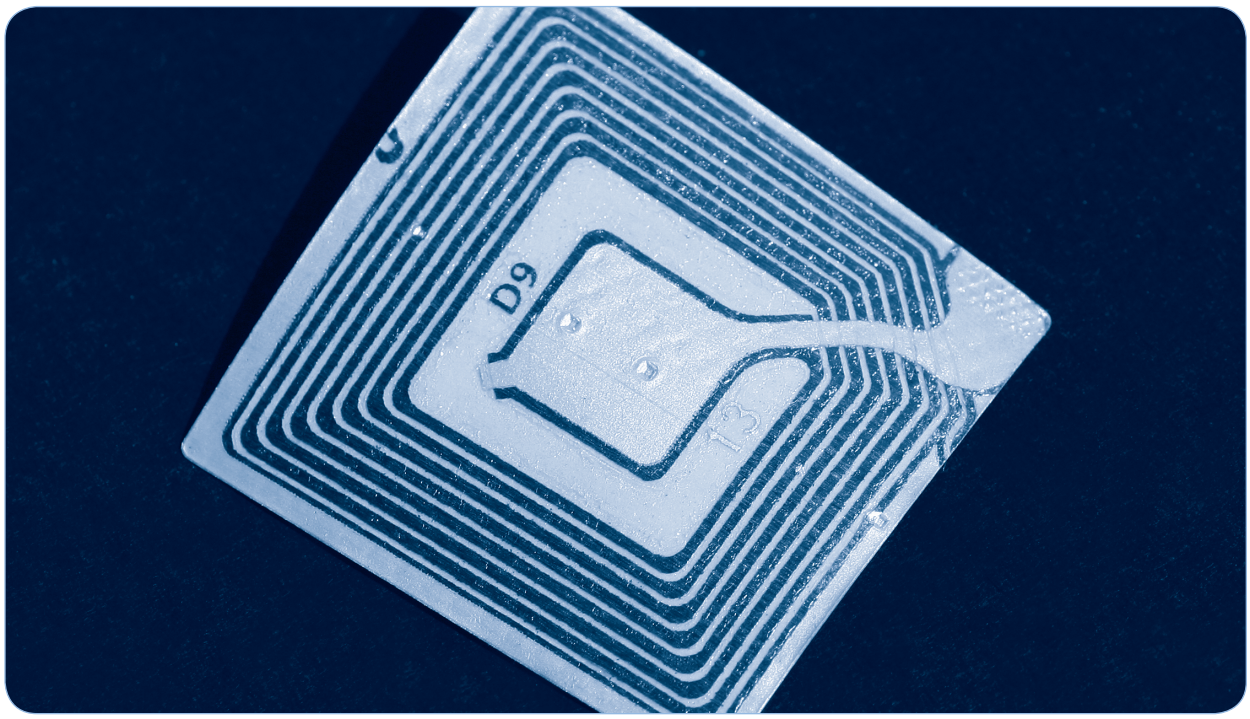
17. Challenges Moving Forward



Like any major new technology system, information technology (IT) brings with it not only vast benefits but also some costs. Automobiles, for example, brought unprecedented mobility and increased productivity but also brought pollution and accidents; overall, though, the benefits of automobiles greatly outweighed the costs. Similarly, IT's benefits have been vast and will continue to be; but at the same time, there are costs associated with IT that the industry itself, government, and citizens should continue to work to minimize.

As discussed below, challenges and costs associated with IT have arisen including issues related to privacy, information security,

information overload, antisocial behavior, the digital divide, and e-waste. Yet the fact that there are challenges and costs associated with IT should not prompt policymakers to try to slow down digital transformation. Doing so would only minimize the significant benefits of a digital society.

As we consider the kind of future we want to live in, it is worth recalling what noted urbanist Lewis Mumford once stated: "Traditionalists are pessimists about the future and optimists about the past." In a world where the opportunities enabled by digital technology are so great, we cannot afford to have our policies guided by "traditionalists," if for no other reason than that the digital future is indeed bright.

Privacy

Perhaps the biggest barrier to more rapid progress toward a digitally enabled society is the fear by some people that this will entail the loss of privacy. Although IT is leading to vastly increased convenience, choice, and empowerment for individuals, some people see an IT-enabled world as a dystopia where our actions will be tracked by corporate or government leviathans. In this view, IT is stripping us of our privacy, exposing our intimate lives to anyone who wants to see them.

To be sure, as more and more information is in digital format, the ease of aggregating information and tying it to individuals has grown. The prospect of vehicle manufacturers installing dedicated short-range communication (DSRC) tags on every car, for example, begs the thorny question of who will have access to the tags, what they can do with the information, and whether access will require consent from the driver or vehicle owner. Will telematics be used to police violations of speed limits, red lights, and stop signs? Will parents be able to observe where and how their kids drive the parents' cars? How about wives and husbands? Will police have access to vehicle travel histories or real time access to vehicle locations for use in criminal investigations?

Civil liberties groups have objected to many applications of data mining because of privacy concerns stemming from the risk of data misuse. Some of their concerns arise from the fact that the government's data-mining projects involve data collected from both the public and private sectors. An additional concern is that the proliferation of digital information will lead to privacy violations by the government.

The suspension of the U.S. government's Total Information Awareness (TIA) data-mining initiative—eventually renamed the Terrorism Information Awareness Program—reflects the degree of public concern with government data-mining programs. The TIA program established by the Defense Advanced Research Projects Agency was discontinued early in the project's lifecycle, so the privacy concerns raised by civil liberties groups were primarily about potential risks rather than actual problems.

Although data mining does not provide investigators a crystal ball, it still can provide insights and clues into investigations. And the benefits of data-mining programs have not yet been fully explored. As data-mining techniques improve, with better data sources, refined algorithms, and lower false-positive rates, societies must continue to find the appropriate balance between privacy and security.

Privacy concerns associated with IT must be taken seriously, but it is important to keep a sense of perspective. Historically, major new technologies have prompted what in hindsight were overblown privacy fears. To cite an example, some people objected to easy-to-use cameras, fearing that individuals' activities would no longer be "private" when walking down the street.[1] Or to cite another example, when transistors were first developed, there was a short-lived privacy scare that everyone would be able to be snooped on using small electronic "bugs." In fact, *Life Magazine* had a headline on it "Insidious Inva-

The answer to many privacy risks is not to ban IT applications entirely, but rather to ensure that the appropriate rules governing privacy and civil liberties are in place and enforced.

sions of Privacy" and Congress even went so far as to hold hearings on the matter.[2] Of course, all this fuss was much ado about very little.

Society has always learned to manage the so-called threats in large part because of the fact that many—but certainly not all—of the concerns raised by privacy activists are hypothetical and speculative.[3] Given the large amount of information in digital format today, it is worth asking how much harm has been done to date. Notwithstanding all the fear and gloom from privacy activists, there simply have not been widespread privacy violations and of the privacy violations that have occurred recently, many have occurred precisely because the information was not in digital form.

The answer to many privacy risks associated with IT is not to ban IT applications entirely or to restrict them in ways that reduce their benefits, as some privacy advocates propose, but rather to ensure that the appropriate rules and practices governing privacy and civil liberties are in place and enforced. In most nations, a series of rules and laws govern how government actors can use personal data, electronic or otherwise. In fact, many of the privacy fears are not about technology, but rather about government access to sensitive information. The fact that more information is in digital form does not change this in any way.

Information Security

As the transition to a digital economy progresses, more and more processes will be completely electronic without paper records. Many people fear that in such an environment, information will not be secure. Moreover, as more people begin routinely storing and exchanging sensitive information online—including credit card numbers, banking information and health records—keeping digital information secure becomes increasingly important.

Fortunately, individuals and organizations are beginning to better understand the importance of implementing good information security practices. In fact, using good cryptographic techniques digital information can be made much more secure and trustworthy than its paper-based equivalent. Strong encryption algorithms help keep information private, digital signatures help authenticate online transactions, and biometric devices help authenticate users. In addition, computers' automatic logging systems help provide insight into security breaches, a safeguard typically only found on computer systems. If an employee snoops through confidential personnel records in the offline world, there is little evidence of this transgression; but if an employee opens a digital file containing the same information on a computer, the user, date, and time of access can all be recorded automatically.

Other security threats and annoyances to computer and Internet users include spam, malware, and phishing. These threats not only impede efforts to develop and deploy online applications but also impose substantial economics costs on individuals, businesses, and government. The worldwide cost of spam—unsolicited commercial e-mail—costs businesses $50 billion worldwide in lost productivity and related expenses.[4] Similarly, the financial impact of malware—malicious software such as viruses, spyware, and adware that runs on a computer without the owner's informed consent—exceeded $13 billion worldwide in 2006.[5] Phishing attacks—in which individuals fraudulently acquire sensitive information such as passwords and credit card information by masquerading as a trustworthy person or business in an electronic communication—has grown considerably, with 144 brands targeted by phishing in December 2007, a drop from the record high of 178 the previous month.[6]

Recognizing these problems, governments, IT companies and IT users are all working together to help reduce the costs of spam, malware, and phishing. Better software engineering practices have led to more robust applications that are more immune to the security flaws of the past. In addition, more secure operating systems have reduced the threat of malicious code corrupting a computer system.

One effect of the reliance on IT for much of modern life is the risk that critical information systems will become unavailable. Economies that rely heavily on connectivity to communicate with their global partners can suffer heavy losses when confronted with network or system outages. Threats to the availability of critical information systems and networks come from both intentional attacks and accidents. In April 2007, for example, following Estonia's removal

of a Soviet-era war memorial, attackers mounted an organized distributed denial of service attack against the websites of government agencies, banks, newspapers, companies, and political parties—causing some of these websites to shut down for hours. Given Estonia's high level of dependence on the Internet for e-commerce and e-government, many feared further attacks could severely disrupt the country. In 2008, two underseas cables were damaged, reportedly by ships' anchors, resulting in a loss of Internet connectivity for large parts of South Asia. Given the importance of outsourcing for countries like India, the loss of these global telecommunication links was a cause for concern.

Just as accidents, crime, and natural disasters cannot be stopped in the real world, neither can engineers prevent all system failures and security breaches in the virtual one. Information security will continue to be an arms race between the good guys and the attackers. At the same time, however, the growing awareness of the importance of information security will lead to better information security controls and practices to reduce risk and improve response in case of a failure. In addition, increased governmental resources devoted to enforcement and prosecution of cybercriminals could help reduce the risks.

Information Overload

When asked to discuss the information society, many people's reaction is that it generates information overload: With access to information 24-7 from a wide variety of sources, some feel that the new digital society has become too rich in information. Saying "turn off your Blackberry" does not assuage many. But in fact, people do have choices, and as people become more used to living in a world where they can always be connected, it is likely that they, and organizations they work for, will develop mechanisms to manage their availability. Already, in fact, some companies are taking steps to limit 24-7 behaviors. The consulting firm PricewaterhouseCoopers has instituted a policy whereby workers accessing the corporate network on weekends are confronted with a message that discourages employees from sending e-mail.[8] Other companies have tried more radical policies such as creating "zero e-mail Fridays."[9]

And in some cases the answer to information overload is simply better technology to manage the flow of information. Numerous tools exist to help users organize their e-mails, documents, photos, and music, find information on their personal computer (PC), and generally be more effective at managing information. A tool released by Google called E-Mail Addict, for example, helps users limit their use of e-mail into more efficient time periods.[10]

Antisocial Behavior

IT has several aspects that raise the risk of facilitating antisocial behavior. First, using IT can be addicting and a form of social escapism. To be sure, high-profile cases—such as an addicted PC gamer in Korea dying after playing at a cybercafé more than 80 hours straight—suggest that for some individuals, PCs can be an antisocial source of escape.[11] But for other individuals, using the Internet can be a social opportunity to meet and interact with new people online. Massive multiplayer online games such as World of Warcraft, for example, connect millions of users from all over the world in an interactive virtual world. Some online games exist specifically for their social element, including the much-hyped virtual world Second Life. Indeed, for every case where IT might lead to isolation, there are many more cases where it enhances community. IT is a very powerful tool for enabling people with similar concerns (e.g., facing the same health problem) or interests (e.g., making films, engaging in political advocacy, enjoying music) to form meaningful online communities.

Second, because Internet communications seem to be a step removed from actual communications with individuals, the normal social graces most people practice when dealing with individuals face to face are sometimes absent. We see this in chat rooms, on blogs and in other digital communications, where insults and recriminations fly freely. We see it in the cyberbullying that goes on among not just some children and teens, but by adults. And the results can be severe, with some children committing suicide in response, and some adults like prominent bloggers Kathy Sierra and Blackamazon taking down their blogs after being attacked or re-

ceiving death threats. Because people have a sense of anonymity on the Internet, they behave in ways that they might otherwise never would if they were face-to-face with someone. Thus, one of the key benefits of the Internet, anonymity, is also a key challenge. It is not clear whether these kinds of antisocial and cruel behaviors are a result of an innate inclination by some people to be cruel and who can now do so with impunity, or whether it is a result of a new medium where new norms of acceptable behavior have yet to fully form.

Whatever the case, there is much more that society can do. Schools and parents can work to educate students on the risks of cyberbullying. Society can more actively take steps against children and teens who engage in such behaviors, behaviors that would never be tolerated in an adult workplace, and if necessary, provide the targets of such bullying with real choices for moving to different educational environments. And those actively engaged in digital forums need to more strongly enforce codes of civilized conduct, and shame and exclude those who practice extreme forms of behavior, just as we do in the offline world.

Finally, because the Internet is essentially a window into whatever individuals want it to be, it means that "bad parts of town" and "bad people" are now just a click away. While some kinds of content is illegal on the Internet in almost all nations (e.g., posting or viewing child pornography) much other content that the average person would view as offensive is not, from violence to racist speech to just plain bad behavior. For adults, this kind of content has always been available in one form or another, the Internet simply makes it easier to access. Short of trying to ban or block certain content (an albeit often difficult technical task), most societies will just have to live with this, and work to ensure that all citizens act in socially beneficial ways.

For children, the task is more complicated. In the old economy, a host of gatekeepers made it much harder for kids to be exposed to this kind of information. Here again, we are at the beginning of this process and as time goes on will learn to deal with it in more effective ways. Technology tools, like Web-filtering tools and monitoring will play a role. Windows Vista, Microsoft's latest operating system, for example, includes parental controls that let parents manage which websites, programs and games their children can access, set time limits on computer usage and generate an activity report of their children's computer usage. Other innovative tools, like Glubble, allow parents to create a "whitelist" of sites their children can access. With Glubble, if a child wants to go to a site not on her approved list, she can simply click a button to request permission from her parents; her request will pop up on her parents' computer—whether they are at home or at work—and her parents can then decide to approve or deny the website remotely.[12] Other content-filtering systems, like Open DNS, allow parents or corporate network administrators to filter content using more than 30 different categories. The Open DNS system relies on an active community of users that can submit tags to classify domain names based on their content.[13] But even with such tools, it is important to teach all children the rules of the road for operating in the digital world. Some schools have now put in place formal curricula to do just that. The Commonwealth of Virginia, for example, now requires all schools to teach Internet safety to their students.[14]

IT is a very powerful tool for enabling people with similar concerns (e.g., health problems) or interests (e.g., politics, films, music) to form meaningful online communities.

Complicating the situation even more is the fact that what is considered bad in one society is considered acceptable in another. When some individuals posted a YouTube video of the king of Thailand morphing into a monkey, for example, many Thai citizens were outraged, seeing this as an egregious insult to their revered monarch. Yet in the United States where the video was posted and hosted, people may not have agreed with the message of the video but they generally agreed with the right of the person to post the video as a fundamental right of free speech.

In the end, the answer is not global censorship; but neither should it be digital anarchy. Each nation should be allowed to manage Internet content in the ways it decides as long as it does not impose costs on those outside its nation, either by trying to require companies outside its nation to manage the content or restricting others outside their nation from viewing the content.

The Digital Divide

As we move to the digital information society, the ability for all citizens to access and understand information will be critical. If only a portion of society has access to information tools such as online learning, electronic health records, and e-government services, then society will move in direction of greater inequality.

Although the risk that some members of society will not be able to participate fully in the digital revolution is real, it is not necessarily a result that is set in stone. The history of virtually all consumer technologies shows the same pattern; early adopters tend to be more educated and wealthier, but as prices fall and ease of use goes up, these technologies become more widespread. We have seen this again and again with technologies like the radio, television, telephone, and, most recently, the cell phone.

If only a portion of society has access to information tools such as online learning, electronic health records, and e-government services, then society will move in direction of greater inequality.

New digital tools are a bit different, however, in that they require a higher level of digital literacy. Learning how to use a cell phone, or at least how to call someone, is pretty straightforward. Learning how to use a computer and the Internet is less so. This suggests governments need to do a better job of facilitating digital opportunity. In South Korea, for example, the government has established digital literacy programs that target population groups that otherwise would be less likely to use the Internet. The "Ten Million People Internet Education Project (2000-2002)" worked to provide Internet education to approximately one-fourth of South Korea's citizens. In addition, the South Korean government has provided subsidies to around 1,000 private training institutes throughout the nation for the purpose of educating housewives. Under this "Cyber 21" program, the government offered 20-hour, week-long courses to housewives for only about $30. In just the first 10 days, 70,000 women signed up for the courses. The Korean Agency for Digital Opportunity and Promotion (KADO) also has a variety of programs to promote digital literacy and access to computers. These include establishing 8,263 local centers where the public can access the Internet for free, distributing free, used personal computers to individuals with disabilities and to those receiving public assistance, and education and training programs for older adults and individuals with disabilities.[16] Initiatives like these help close the digital divide and promote more equal digital opportunity.

Cybertribalism

In the old economy, people had significantly fewer choices than they do in the digital economy. And although the old economy may have limited individual choices, many argue that it promoted social cohesion. If everyone got the news from the same media outlets and got TV from the same three channels, it was easier to maintain a coherent society.

There is no doubt that the digital economy provides a vast array of choices—a situation that, by its very nature, means that individuals in a particular nation may be getting different information. But at the same time, individuals' ability to get information on their own from a variety of sources—and not mediated by powerful elites seeking to control a docile population—is breaking down more rigid, authoritarian societies.

Moreover, the very nature of the digital society is breaking down barriers across groups and nations,

making people more and more citizens of the world. Because of the Internet, individuals are able to connect to others around the globe they might otherwise never encounter. As a result of IT, it is much easier to communicate with people from other nations and groups, to see and understand what is happening to them, and to essentially live in a cyber global village.

E-Waste

Although IT underpins advanced recycling applications, the disposal of IT hardware has lately become a cause for concern due in large part to toxic compounds, including heavy metals, contained in most IT hardware, which, if not properly disposed of, can leech into groundwater and the surrounding environment. The problem is not helped by the fact that IT equipment rapidly becomes obsolete because it improves so quickly, creating successive generations of so-called "e-waste." In fact, the United States generates between 1.9 and 2.2 million tons of electronics waste every year, 400,000 tons of which are recycled (2005 data).[17] Nor is the United States alone in generating large amounts of e-waste; it is estimated that Germany alone produced 1.1 million metric tons of e-waste in 2005.[18] One estimate pegs worldwide e-waste at 50 million tons annually.[19]

Governments and IT equipment manufacturers are tackling the environmental problems created by hazardous e-waste in two ways. First, companies are working to limit the use of hazardous materials in IT equipment, often in cooperation with government guidelines. Second, companies and governments are working together to recycle unwanted equipment. Many companies, including IBM, Dell, and HP, offer programs in which consumers can ship used equipment to them to be recycled for a small fee. Nonetheless, the extent to which consumers use such programs remains unclear, with some experts arguing that participation is quite limited.[20]

Various policies have been used by national and subnational governments to promote e-waste recycling. As of July 2008, 15 states in the United States had signed into law electronics recycling laws. The state of California, for example, began collecting a small fee for e-waste recycling from consumers in 2005 for every sale of a covered electronic device, including laptops and monitors. The money collected by the state is set aside in a fund used to offset the costs of proper collection and disposal of these products, which are no longer accepted with other household trash collection.[21] Other states have turned to a producer responsibility framework that requires IT manufacturers to assume the financial responsibility for recycling their products. The intent of this approach is to give manufacturers an incentive to make products that are cheaper to recycle (and have less toxic material), although its effectiveness has not yet been determined.

If not handled properly, the recycling process for IT products can be dangerous. Seventy percent of the world's recycled e-waste ends up in China, where, according to a recent study, it is often subject to improper handling, resulting in the leeching of heavy metals into the local environment. Recyclers disassemble discarded cell phones, televisions, computers, and other e-waste items in order to reuse the valuable metals contained within them, but they often do so without adequate safeguards for either personal or environmental safety. In one center of e-waste recycling, the town of Guiyu in southeastern China, for example, researchers have found that the community is highly contaminated with dangerous heavy metals. Dust from the Guiyu's roads contains lead levels 330 times and 371 times higher than lead concentrations in nearby communities that do not recycle e-waste.[22] Concentration levels for other metals, including zinc, nickel, and copper, are similarly elevated.

Clearly, discarded computer parts require delicate handling and proper disposal for the sake of both human health and the surrounding environment. Although the e-cycling chain in some nations appears to have inadequate safeguards to protect human health and the environment, electronic waste can be disposed properly, especially with the help of new and emerging recycling technologies. One example of a recently developed recycling process is an automated process for recycling printed circuit boards (computer innards that contain a wide array of heavy metals) that renders the components into salvageable bits of metal and plastic in an environmentally responsible way.[23] The recycling technique employs a two-step crushing process and magnets to

separate effectively the various metals. This approach represents a significant environmental and efficiency improvement over other popular mechanical and chemical processes.[24]

In sum, although the sheer volume of e-waste presents an environmental challenge given its toxic nature, it appears that public awareness, governmental and corporate initiatives, and recycling techniques are finally beginning to catch up to scope the of the problem.

Conclusion

It has now been slightly more than a decade since the Internet became a mass phenomena and the digital economy began to take off. The United States, and indeed the world, have benefited greatly from the changes, with faster productivity and income growth, more innovation, higher quality products and services, and increased opportunity and convenience for hundreds of millions of IT users around the globe.

It is not clear how long IT will power economic growth, but it seems likely that for at least the next decade or two, IT will remain the engine of growth. The opportunities for continued diffusion and growth of the IT system appear to be strong. Many sectors of the economy, including health care, education, and government, have only begun to tap the benefits of IT-driven transformation. Adoption rates of e-commerce for most consumers, while rapid, are still relatively low. And the emergence of new technologies such as radio-frequency identification (RFID), wireless broadband, speech recognition programs, and others will enable still new IT applications.

In short, although the emerging digital economy has produced enormous benefits, the best is yet to come. The job of policymakers in developed and developing nations alike is to ensure that the policies and programs they put in place actively spur digital transformation so that all their citizens can fully benefit.

Endnotes

1. For a modern day example of misplaced privacy fears, see Daniel Castro, "I Spy a Luddite: Why the Lawsuit over Google Street View is Absurd," Information Technology and Innovation Foundation, Washington, D.C., April 25, 2008 <www.itif.org/index.php?id=141> (accessed August 10, 2008).

2. John Neary, "Electronic Snooping—Insidious Invasions of Privacy," *Life Magazine*, May 20, 1966. <www.bugsweeps.com/info/life_article.html> (accessed August 10, 2008).

3. Robert D. Atkinson, "RFID: There's Nothing to Fear Except Fear Itself," remarks at the 16th Annual Computer, Freedom and Privacy Conference, Washington, D.C., May 4, 2006 <www.itif.org/index.php?id=65> (accessed August 10, 2008).

4. Gregg Keizer, "Spam Costs Businesses Worldwide $50 Billion" *InformationWeek*, February 23, 2005 <www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=60403016> (accessed August 10, 2008).

5. Computer Economics, Inc., "Annual Worldwide Economic Damages from Malware Exceed $13 Billion," Irvine, California, June 2007 <www.computereconomics.com/article.cfm?id=1225> (accessed August 9, 2008).

6. Anti-Phishing Working Group, "Phishing Activity Trends," December 2007 <www.antiphishing.org/reports/apwg_report_dec_2007.pdf> (accessed August10, 2008).

7. Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, May 17, 2007 <www.guardian.co.uk/world/2007/may/17/topstories3.russia> (accessed August 10, 2008).

8. "Managing," *BusinessWeek.com*, May 8, 2008 <www.businessweek.com/magazine/content/08_20/c4084managing073122.htm?chan=search> (accessed August 10, 2008).

9. Michelle Kessler, "Fridays Go from Casual to E-Mail-Free," *USA Today*, October 5, 2007 <www.usatoday.com/tech/techinvestor/corporatenews/2007-10-04-no-email_N.htm> (accessed August 10, 2008).

10. L. Gordon Crovitz, "Unloading Information Overload," *Wall Street Journal*, July 7, 2008: A11 <online.wsj.com/public/article_print/SB121538872997031145.html> (accessed August 10, 2008).

11. Caroline Gluck, "South Korea's Gaming Addicts," *BBC News World Edition*, November 22, 2002 <news.bbc.co.uk/2/hi/asia-pacific/2499957.stm> (accessed August 10, 2008).

12. Glaxstar, Inc., Glubble Webpage, 2008 <www.glubble.com/features> (accessed August 10, 2008).

13. OpenDNS, "Content Filtering," San Francisco, California, 2008 <www.opendns.com/features/content_filtering/> (accessed August 10, 2008).

14. Office of Educational Technology, Virginia Department of Education, "Guidelines and Resources for Internet Safety in Schools," n.d. <www.doe.virginia.gov/VDOE/Technology/OET/internet-safety-guidelines.shtml> (accessed August 10, 2008).

15. Jack Schofield, "Miracle Workers: In Just Five Years, South Korea Has Shown the World What the Broadband Future Looks Like," *The Guardian*, October 17, 2002 <www.guardian.co.uk/internetnews/story/0,7369,812943,00.html> (accessed August 10, 2008).

16. "Introduction of KADO (Korea Agency for Digital Opportunity and Promotion)," n.d. <unpan1.un.org/intradoc/groups/public/documents/UNPAN/UNPAN028063.pdf > (accessed August 10, 2008).

17. U.S. Environmental Protection Agency, eCycling Webpage, updated July 22, 2008 <www.epa.gov/ecycling/> (accessed August 10, 2008).

18. Empa Switzerland, "International E-Waste Generation," *Swiss E-Waste Guide*, 2008 <ewasteguide.info/international_e_waste_generation> (accessed August 10, 2008).

19. "Elevated Concentrations of Toxic Metals in China's E-Waste Recycling Workshops," *ScienceDaily*, April 1, 2008 <www.sciencedaily.com/releases/2008/03/080331092500.htm> (accessed August 10, 2008).

20. Zachariah Mully, "The E-Waste Tsunami," SmartBrief Blog on the Milken Institute Global Conference 2006, April 24, 2006 <smartbrief.blogspot.com/2006/04/e-waste-tsunami_24.html> (accessed August 10, 2008).

21. "What's Up With This Fee On My Receipt," *eRecycling.org*. <www.erecycle.org/index.htm>.

22. Anna O. W. Leung et al., "Heavy Metals Concentrations of Surface Dust from e-Waste Recycling and Its Human Health Implications in Southeast China," *Environmental Science & Technology* 42 (7), 2008, 2674-2680 <pubs.acs.org/cgi-bin/abstract.cgi/esthag/2008/42/i07/abs/es071873x.html>.

23. Jia Li et al., "Recycle Technology for Recovering Resources and Products from Waste Printed Circuit Boards," *Environmental Science & Technology* 41 (2007): 1995 <pubs.acs.org/cgi-bin/sample.cgi/esthag/asap/pdf/es0618245.pdf> (accessed August 10, 2008).

24. Jia Li et al., 2007.

This chapter is from the publication:

Digital Quality of Life: Understanding the Personal and Social Benefits of the Information Technology Revolution
by Dr. Robert D. Atkinson and Daniel D. Castro

To learn more or to download a copy of the complete report, please visit the Information Technology and Innovation Foundation online at www.innovationpolicy.org.

About the Information Technology and Innovation Foundation

ITIF is a non-profit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington DC and in the states. Recognizing the vital role of technology in ensuring American prosperity, ITIF focuses on innovation, productivity, and digital economy issues.

Technological innovation, particularly in information technology, is at the heart of America's growing economic prosperity. Crafting effective policies that boost innovation and encourage the widespread "digitization" of the economy is critical to ensuring robust economic growth and a higher standard of living. However, as in any new and changing situation, policymakers have varied awareness of what is needed and what will work. In some cases legislators have responded to new and complex technology policy issues with solutions more suited for the old economy. And as the innovation economy has become increasingly important, opposition to it from special interests has grown. Finally, the excitement that the press, pundits and decision makers showed toward the information technology (IT) revolution in the 1990s has all too often been replaced with an attitude of "IT doesn't matter." It is time to set the record straight—IT is still the key driver of productivity and innovation.

As a result, the mission of the Information Technology and Innovation Foundation is to help policymakers at the federal and state levels to better understand the nature of the new innovation economy and the types of public policies needed to drive innovation, productivity and broad-based prosperity for all Americans.

ITIF publishes policy reports, holds forums and policy debates, advises elected officials and their staff, and is an active resource for the media. It develops new and creative policy proposals to advance innovation, analyzes existing policy issues through the lens of advancing innovation and productivity, and opposes policies that hinder digital transformation and innovation.

To find out more about the Information Technology and Innovation Foundation, please contact us at 1250 I Street, NW, Suite 200, Washington, DC 20005.

E-mail: mail@itif.org. Phone: (202) 449-1351.
Web: www.innovationpolicy.org