

Key Terms

biotechnology, 263	e-business, 267	social networking, 271
blog, 272	information phase, 263	spam, 273
cellular telephones, 269	Internet, 266	technology, 262
cyberchondriacs, 279	m-commerce, 269	unsolicited commercial
cyberspace, 263	phishing, 274	e-mails, 273
digital divide, 280	QR code, 269	vlog, 273
digital medical records, 279	semantic phase, 263	

Internet Resources

www.antiphishing.org	Anti-Phishing Working Group
www.bio.org	Biotechnology Industry Organization
www.computerworld.com	Computer World
www.digitaldividenetwork.org	Digital Divide Network
www.ebizmba.com	eBiz/MBA
www.ecommercetimes.com	E-Commerce Times
www.foresight.org	Foresight Institute
www.internetsociety.org	Internet Society
www.networkworld.com	Network World
www.pewinternet.org	Pew Internet and American Life Project
socialmediatoday.com	Social Media Today
technorati.com	Technorati
www.whatisocialnetworking.com	Social Networking

Discussion Case: *How Protected Is Your Online Privacy?*

"Solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon [personal] privacy, subjected [individuals] to mental pain and distress. In this, as in other branches of commerce, the supply creates demand."

This quotation appeared in the *Harvard Law Review*. Besides the sobering sentiment expressed, the more startling fact is that it was written in 1890, more than 120 years ago! Technology, whether it is in the 1890s or 2010s, can violate our sense of privacy as individuals. Consider these examples:

- Malicious programs launched by hackers spread through Facebook and Twitter accounts in 2009, taking over people's accounts and sending out messages to the users' friends and followers. One user found out five days later that his account had been sending out lingerie ads to all of his professional acquaintances.
- When Google introduced *Buzz*, its answer to Facebook and Twitter, in 2010, users found themselves with an instant, and in many cases unwelcome, collection of "friends,"

automatically selected by Google from their e-mail contact lists. The users complained that their e-mail information contained names of personal physicians and illicit lovers, as well as the identities of whistle-blowers and antigovernment activists, most of whom would not want their identities made available to these “friends.”

- In 2010, a *Wall Street Journal* investigation discovered that Facebook regularly transmitted identifying information—providing access to peoples’ names and in some cases their friends’ names—to dozens of advertising and Internet tracking companies. These firms used the information to build user profiles to market new apps or games. The use of apps was a growing source of revenue for Facebook since it sold virtual currency that could be used to pay for games. This activity affected tens of millions of Facebook users, including people who set their profiles to Facebook’s strictest privacy settings.
- The *Wall Street Journal* probe revealed that MySpace also had been transmitting information to advertising companies that could be used to identify users. Users’ information was sent, without their knowledge, once they clicked on ads on the MySpace website. At that time, MySpace had 58 million visitors monthly in the United States.

As this epidemic of privacy violations became public, many organizations, including the social network companies and the U.S. government, pledged to correct the situation. Some businesses, such as Microsoft and McAfee, saw this situation as an opportunity to offer online consumers software to protect them from online monitoring. Other companies offered users a commission every time their personal details were shared with marketing companies. “Data is a new form of currency,” said a technology executive. The reasoning seemed to be that if the online advertising industry was bringing in \$26 billion a year in sales from accessing this information, the consumers should share in the profits.

Apple, Facebook, and Google also took the offensive and created plans to better protect their customers. In 2011, Apple announced it would no longer automatically track an iPhone’s location, but download a subset, or cache, of the database from each phone. This limited access to data prohibited Apple from locating the user who was using WiFi or a cell phone. While Apple needed to track its users to provide better service—for example, to identifying WiFi hotspots and cell towers—the new software would reduce the size of the database cached on the phone, cease backing up the cache, and delete the cache entirely when the location tracking feature was turned off.

Facebook acknowledged the security vulnerabilities found in the *Wall Street Journal* investigation and reported that they had addressed the problem in 2011. “We’ve conducted a thorough investigation, which revealed no evidence of this issue resulting in user’s private information being shared with unauthorized third parties,” the company stated. “[Facebook has a] strong policy enforcement and technical measures that allow us to quickly catch and take action against suspicious behavior on the platform.”

Google also was caught up in the *Wall Street Journal* investigation. It had allegedly used a special computer code that tricked the Safari web-browsing software to allow Google to monitor users’ activities. Safari was designed to block such tracking by default. Google reported in 2012 that it had disabled its code after being contacted by the *Wall Street Journal*, although the company maintained that “The [Wall Street] Journal [investigation] mischaracterize[d] what happened and why.”

Finally, legislators also took action. Senators John Kerry and John McCain introduced a “privacy bill of rights,” which included a “do not track” provision patterned after the “do not call” law that allowed people to block telemarketing calls to their phone. The proposed law would impose strict rules on companies that gather personal data, including requiring that people be given the right to access data collected about them and to block the

information from being used or distributed. Although the Internet industry had resisted legislative controls for more than a year, a coalition of Internet giants joined the White House in support of the Kerry-McCain “do not track” provision. This provision allowed for a button to be embedded in most web browsers to give people greater control over the personal data collected about them.

Yet, some experts questioned whether these measures would be enough. They pointed to powerful new methods of tracking, such as ones found on MSN.com and Hulu.com, that were almost impossible for computer users to detect. These new techniques were called “supercookies.” These supercookies were similar to a traditional cookie, a small file routinely installed on users’ computers to track their activities online, but were capable of recreating users’ profiles after people deleted regular cookies.

Sources: “Technology Outpaces Privacy [Yet Again],” *The New York Times*, December 11, 2010, www.nytimes.com; “Crooks Hijack Facebook Accounts, Injuring Dignity,” *The New York Times*, December 14, 2009, www.nytimes.com; “Critics Say Google Invades Privacy with New Service,” *The New York Times*, February 13, 2010, www.nytimes.com; “Facebook in Privacy Breach,” *The Wall Street Journal*, October 18, 2010, online.wsj.com; “MySpace, Apps Leak User Data,” *The Wall Street Journal*, October 22, 2010, online.wsj.com; “Internet Gets New Rules of the Road,” *The Wall Street Journal*, December 22, 2010, online.wsj.com; “Web’s Hot New Commodity: Privacy,” *The Wall Street Journal*, February 28, 2011, online.wsj.com; “Apple Plans Fix for iPhone Location Data,” *The Wall Street Journal*, April 27, 2011, online.wsj.com; “Facebook Security Flaw Exposed User Accounts,” *The Wall Street Journal*, May 11, 2011, online.wsj.com; “Google’s iPhone Tracking,” *The Wall Street Journal*, February 17, 2012, online.wsj.com; “Web Firms to Adopt ‘No Track’ Button,” *The Wall Street Journal*, February 23, 2012, online.wsj.com; “Senators Offer Privacy Bill to Protect Personal Data,” *The Wall Street Journal*, April 13, 2011, online.wsj.com; “F.T.C. Backs Plan to Honor Privacy of Online Users,” *The New York Times*, December 1, 2010, www.nytimes.com; and “Latest in Web Tracking: Stealthy ‘Supercookies,’” *The Wall Street Journal*, August 18, 2011, online.wsj.com.

Discussion Questions

1. How much privacy should people expect when using a social networking site or going online for information, shopping, or other tasks?
2. Who should be responsible for protecting Internet users’ personal information? In your response, please address the appropriate role of the government, business, and individuals.
3. Should consumers share in the revenue generated from sales created by accessing the personal information from social networking and other Internet sites?
4. Do you believe there is a conflict between the economic interests of companies such as Facebook, MySpace, or Google, and their obligation to protect the personal information of their users? If you were an executive of one of these companies, how would you resolve that conflict?