Issue: Technology and Business Ethics

Technology and Business Ethics

By: Patrick Marshall

Pub. Date: February 15, 2016
Access Date: October 24, 2024
DOI: 10.1177/237455680204.n1
Source URL: https://businessresearcher.sagepub.com/sbr-1775-98200-2717708/20160215/technology-and-business-ethics

Executive Summary

Rapidly advancing technologies such as big data analytics offer potentially great benefits to companies and consumers, but experts warn that modern technology also has a downside: It can give companies seeking a competitive edge the tools to engage in illegal or unethical practices. Because digital devices—from the sensors and computers that control the inner workings of automobiles to code that tracks individuals' activities on the Internet—are powered by software that is inherently invisible, consumers and regulators are often in the dark about the data that companies are collecting and how they are using it. Industry groups and outside observers disagree about what should be done. The former argues self-regulation is sufficient while the latter seeks tough regulation and increased ethics training in business schools and companies. Among the questions being debated: Should the uses of big data be more tightly controlled? Should there be limits on employers' monitoring of employees? Is software too open to abuse?

Overview

Volkswagen, which admitted last year that it had installed software in 11 million diesel automobiles designed to alter emissions tests, faces fines and lawsuits that could run into the billions of dollars. (Adam Berry/Getty Images)

Months after Volkswagen publicly admitted in August 2015 that it had installed software in 11 million diesel automobiles designed to deceive emissions tests, the public remains in the dark about just who was responsible.

Michael Horn, head of Volkswagen's American division, told Congress on Oct. 8 that neither Volkswagen's supervisory board nor its top executives ordered the installation of devices that could sense when they were being tested and then change the vehicles' performance to improve results. "This was not a corporate decision," Horn said. "This was something individuals did." [1]

While it is not yet known who was behind the decision to deploy deceptive software, it is growing clear that the company is paying a huge price for the scandal.

Indeed, as a result of sharply lower sales, in late October Volkswagen reported its first quarterly loss in at least 15 years. [2] And even though the company has denied the involvement of upper management, its CEO was forced to resign and five high-ranking executives have been suspended. Volkswagen reportedly has set aside $7.3 billion to bring affected vehicles into compliance with emissions standards, and the company faces an uncertain amount of fines and lawsuits that experts expect to run into the billions of dollars. [3]

Volkswagen is not alone in embedding legally or ethically questionable practices in complex technologies. The Internet is riddled with software with hidden functionality. For example, AVG, a company that offers users free antivirus protection, recently acknowledged that it tracks users' browsing and search activity and that it may sell that information to advertisers. [4] AVG defended the practice by noting that it is disclosed in the consumer contract that users accept—even if they don't read it—when installing the software.

The power and opacity of modern technology—from software to surveillance tools and big data analytics—is both a boon to business and a temptation to companies to engage in illegal or unethical practices to gain an edge in a competitive global economy. The growth in these practices has occurred so rapidly that it is outpacing the law. At the same time, because digital devices are powered by software that is inherently complex and non-transparent, consumers and regulators alike generally are in the dark about just what data is collected and the purposes to which it is being put.

"What happens behind the screen is unknown to almost everyone," says Penny Duquenoy, a principal lecturer at Middlesex University, London, who specializes in the ethical implications of information technology (IT). "The fact that technology is opaque gives people the opportunity to exploit it."

According to Duquenoy, digital technologies present a special challenge for business ethics because they are opaque not only to consumers but also to managers and corporate executives. "The IT people are coming from a different place and use a different language," she says. "You need some technical people at board [of directors] level to get across what happens with technology."

Kirsten Martin, assistant professor of strategic management and public policy at George Washington University's School of Business, agrees. "I do think there is a problem in that the number of people who know how to code is very small," she says. "I do think that impacts how many questions an executive or an account manager will ask because they feel stupid."

The situation puts an extra burden on companies—rather than lawmakers or regulators—to follow ethical practices in implementing new technologies, says Arthur Schwartz, general counsel of the National Society of Professional Engineers.

“I don't think the laws and regulations ever keep up,” Schwartz says. “We need to train engineers and other learned professions about the ethical implications of their activities. And it's not just something to study in college. It needs to be ongoing.”

The Volkswagen situation illustrates how technology allows unethical and illegal actions to occur almost invisibly and “with comparatively few people being in the accountability line,” says Ken Goodman, director of the University of Miami's Miller School of Medicine Institute for Bioethics and Health Policy and co-director of the University of Miami Ethics Programs.

“In the next business ethics seminars [after the Volkswagen scandal], we are going to say, ‘Why did they do it? Do they not think they would get caught? Were they not concerned?’ ” Goodman says.

Whether it's in the board room or the engineering labs, digital technologies present hurdles for ethical business practices, says Tony Wasserman, professor of software management practice at Carnegie Mellon University. “There have always been people who live on the edge of ethics and propriety,” he says. “It's just that now we have created a whole new set of opportunities for the people who want to push the boundaries.”

Possibilities for abuse abound. “Sophisticated monitoring software and hardware allow businesses to conduct basic business transactions, avoid liability, conduct investigations and, ultimately, achieve success in a competitive global environment,” according to Corey Ciocchetti, professor of business ethics at the University of Denver. At the same time, Ciocchetti wrote, “This trend is problematic because excessive and unreasonable monitoring can: (1) invade an employee's reasonable expectation of privacy, (2) lead employees to sneak around to conduct personal activities on work time, (3) lower morale, (4) cause employees to complain and, potentially, quit and (5) cause employees to fear using equipment even for benign work purposes.” [5]

Despite the challenges, surveillance technologies have been used widely. A survey by the American Management Association found:

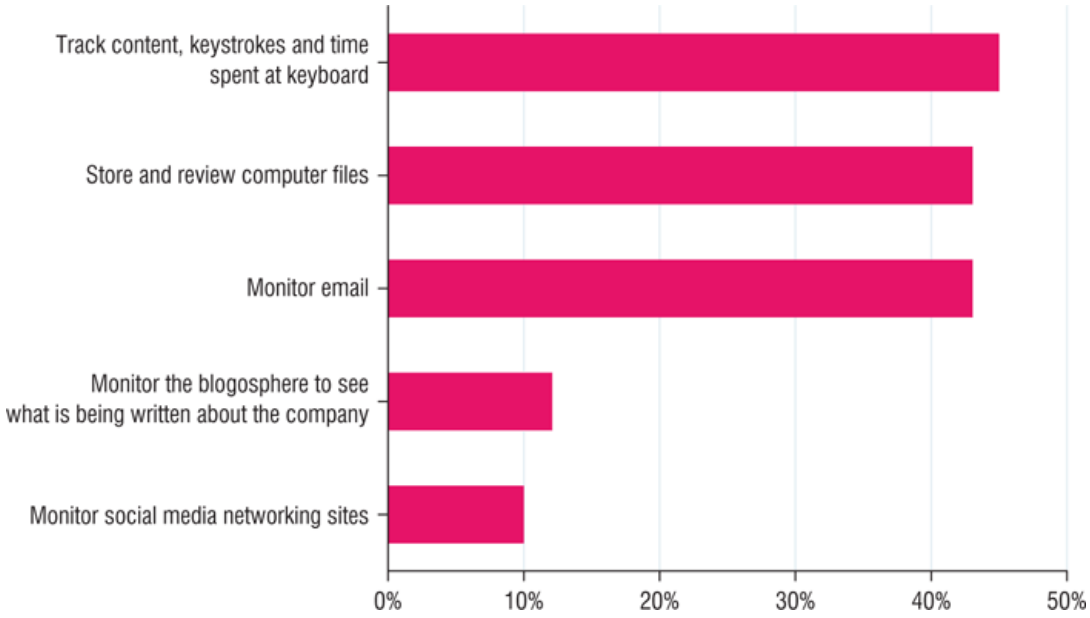
- 45 percent of companies track employees’ keystrokes, and time spent at the keyboard.
- 43 percent of companies store and review computer files.
- 12 percent of companies monitor the blogosphere for comments about the company.
- 10 percent of companies monitor social networking sites. [6]

Business ethicists and privacy advocates also are concerned about the need to establish standards for appropriate uses of consumer data that companies collect.

“The ongoing collection of personal information in the United States without sufficient privacy safeguards has led to staggering increases in identity theft, security breaches, and financial fraud,” Marc Rotenberg, executive director of the nonprofit Electronic Privacy Information Center (EPIC), told Congress in April 2014. [7]

Nearly Half of U.S. Companies Track Employees’ Browsing

Percentage of employers that …



Note: Based on survey of 304 U.S. companies from 2007.

Source: "The Latest on Workplace Monitoring and Surveillance," American Management Association, updated Nov. 17, 2014, http://tinyurl.com/guk2q3k

Forty-five percent of American companies track employees' browsing content, keystrokes and time spent at the computer, according to a 2007 survey by the American Management Association. At that time, while about four in 10 companies stored and reviewed employee computer files or monitored their email accounts, only about one-tenth monitored blogs or social media for coverage of their companies.

And big data analytics—the use of software to analyze huge amounts of collected data to reveal hidden patterns—has led to privacy incursions. One often-cited example of the unexpected consequences of such data analysis was Target's use of data about one customer's purchase patterns to determine that she was pregnant. The retail chain began sending her coupons for baby products. The problem was that she had not yet told her family that she was pregnant. [8]

According to EPIC, "By 'connecting the dots' between different, disparate datasets, or even by analyzing data from the same dataset that on its face does not seem to have any connection, companies can infer characteristics about people that they might not otherwise wish to be made public, or at least not wish to share with certain third parties." [9]

In fact, in light of the power of big data and its potential for abuse, an analyst for Gartner, a technology consulting firm, told a conference in October 2015 that by 2018, half of business ethics violations will result from improper use of big data analytics. [10]

At least some experts are hopeful that companies are coming to realize the importance of taking steps to ensure the ethical use of digital technologies.

"Some companies are beginning to realize that there is a benefit to trying to encourage transparency and being forthcoming," Schwartz says.

In 2012, the Business Roundtable, an influential Washington, D.C.-based group of corporate CEOs that advocate for pro-business policies, formed a new effort on innovation and technology as part of the group's Institute for Corporate Ethics. The goal of the effort, the Business Roundtable said on its website, was to develop "leading thinking and practices for managing the ethical challenges that emerge from technological advancement and innovation." [11]

According to George W. Reynolds, professor of business at Strayer University and author of a textbook on information technology ethics, one way to respond is an increased focus on ethics training, both in business schools and in companies. He cited research that "86 percent of the employees in companies with a well-implemented ethics and compliance program are likely to perceive a strong ethical culture within the company, while less than 25 percent of employees in companies with little to no program are likely to perceive a culture that promotes integrity in the workplace." [12]

Others have proposed increasing professionalization of IT workers, including certification that requires adherence to ethical codes. "The IT industry is not regulated in the same way as lawyers and doctors," notes Duquenoy. "If lawyers or doctors transgress, they lose their license and are not allowed to practice. That doesn't apply when it comes to information technology engineers or software engineers."

Some experts have argued that whistleblower protections for private-sector employees need to be improved. Employees are more likely to take a stand against unethical behaviors if they don't fear losing their jobs as a result. [13]

“I think we definitely need a culture of whistleblowing,” says Karen Sandler, executive director of the Software Freedom Conservancy, a nonprofit organization based in Brooklyn that advocates the use of open-source software.

As technologists, managers and ethicists consider the implications of information technology for businesses, here are some of the issues under debate:

Weighing the Issues

Should the uses of big data be more tightly controlled?

Big data is big business. IDC, a market research firm, estimates that the big data technology and services market will grow by more than 26 percent a year to reach $41.5 billion by 2019. [14]

The amount of data collected on U.S. citizens by private-sector companies is also huge. According to a 2014 report by the Federal Trade Commission, one data broker—a company that collects, combines and analyzes data—by itself has information on 1.4 billion consumer transactions. Another data broker cited by the commission adds 3 billion records each month to its databases. Yet another data broker has 3,000 data “segments”—individual categories of data—on nearly every consumer in the United States. [15]

“The scale of the Big Data Revolution is such that all kinds of human activities and decisions are beginning to be influenced by big data predictions, including dating, shopping, medicine, education, voting, law enforcement, terrorism prevention, and cybersecurity,” wrote law professor Neil M. Richards and CenturyLink executive Jonathan H. King. “Many of the most revealing personal data sets such as call history, location history, social network connections, search history, purchase history, and facial recognition are already in the hands of governments and corporations. Further, the collection of these and other data sets is only accelerating.” [16]

At the same time, the data brokerage industry remains largely unregulated, and most consumers have little idea about the types and amount of data being collected about them.

“Since consumers generally do not directly interact with data brokers, they have no means of knowing the extent and nature of information that data brokers collect about them and share with others for their own financial gain,” according to a recent staff report for the Senate Committee on Commerce, Science and Transportation. [17]

As a result, some legislators and privacy groups have been calling for legislation to limit what data companies can collect and what they can do with it after collecting it.

Among others, the Center for Democracy & Technology, a Washington, D.C.-based nonprofit research and advocacy group, has called for passage of general national privacy legislation to regulate companies’ use of data. “Most industrialized democracies, except the United States, have such a law,” says Chris Calabrese, CDT's vice president for policy. However, because the Republican-controlled Congress generally takes a dim view of imposing limits on business in such a fashion, he acknowledges, “It's a tough road at the federal level.”

“Far too many organizations collect detailed personal information and use it with too little regard for the consequences,” wrote the Electronic Privacy Information Center in response to a request for information from the federal Office of Science and Technology Policy. “The current Big Data environment is plagued by data breaches and discriminatory uses of predictive analytics.” [18]

Tracking of information by data brokers is more worrying than surveillance by the U.S. government, according to now-former Sen. Jay Rockefeller, D-W.Va., who in 2013 chaired a Senate committee that looked into the brokerage industry. [19]

Jay Rockefeller: Data brokers pose a big threat to privacy. (Alex Wong/Getty Images)

The committee's report found that data brokers “operate behind a veil of secrecy,” and concluded, “It is important for policymakers to continue vigorous oversight to assess the potential harms and benefits of evolving industry practices and to make sure appropriate consumer protections are in place.” [20]

The FTC has gone further, calling for legislation that would, among other things:

- Require data brokers to give consumers access to their data.
- Require opt-outs, so that consumers can prevent use of their data.
- Require retailers and other “consumer-facing entities” to provide prominent notice of data sharing, as well as an opt-out.

However, any such legislation will need to have teeth, because the FTC has long made such recommendations, according to Nate Cardozo of the Electronic Frontier Foundation, a San Francisco-

based civil liberties advocacy group. “The FTC says that we should have choice about whether to be tracked and about what companies do with the information,” Cardozo says. “If that was the way the world actually worked, consumer privacy advocates around the country would be out of a job. But that's not the way the world works.”

Data brokers stress the benefits of the data and analytic tools they deliver to companies and to consumers.

“Marketing data, in particular, brings lower prices and greater convenience to consumers by strengthening competition,” Tony Hadley, Experian's senior vice president for government affairs, told Rockefeller's committee. As one of the three big credit reporting companies, Experian is an active data brokerage. “Both large and small businesses rely on data to make their marketing efforts more efficient and to identify new customers.… Consumers also benefit from receiving relevant advertising offers that they are more likely to value and use.” [21]

Additional restrictions are unnecessary, Hadley said. “Experian shares data responsibly—by carefully safeguarding compliance with all privacy and consumer protection laws and industry self-regulatory standards, advancing and observing industry best practices, and establishing and monitoring adherence to our own corporate policies and practices,” he told the committee.

Jerry Cerasale, senior vice president of government affairs at the Direct Marketing Association, a New York City-based group that represents marketing companies, also argued to the committee that industry self-regulation is sufficient. “Some policymakers have raised concerns that data collected for advertising purposes could be used as a basis for employment, credit, health care treatment, or insurance eligibility decisions,” he said. “In fact, these are hypothetical concerns that do not reflect actual business practices. Nevertheless, industry has stepped forward to address these concerns by expanding its codes of conduct to clarify and ensure that such practices are prohibited and will never occur.” [22]

Experian and the Direct Marketing Association did not respond to interview requests for this report.

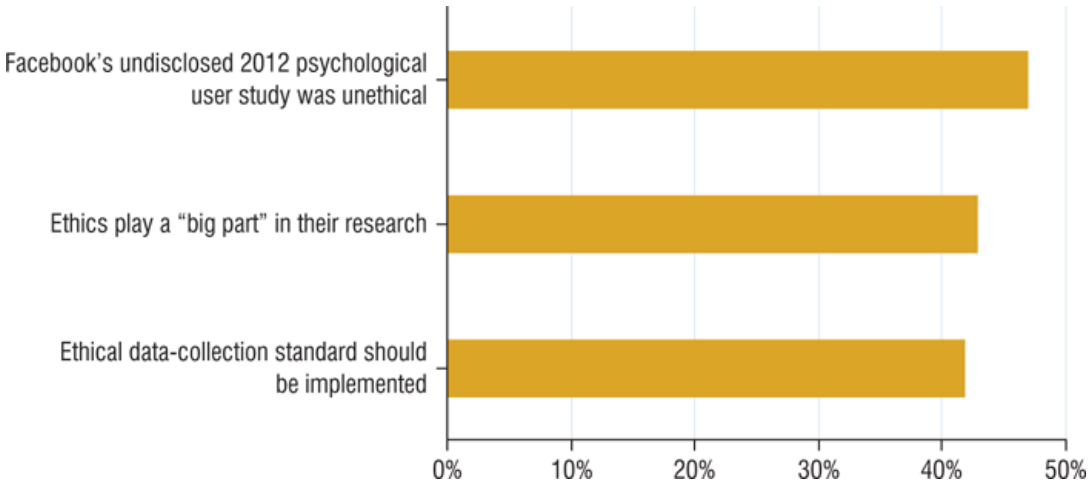
Should there be limits on employers’ monitoring of employees?

Companies have monitored employee telephone and computer use for as long as there have been telephones and computers. But recent advances in digital technologies have made it possible to monitor employee behavior, and even attitude, to an unprecedented degree.

The New York Times last year highlighted a situation involving Jim Sullivan, a waiter at a Dallas restaurant whose actions came under scrutiny “not by the prying eyes of a human boss, but by intelligent software. The digital sentinel, he was told, tracked every waiter, every ticket, and every dish and drink, looking for patterns that might suggest employee theft. But that torrent of detailed information, parsed another way, cast a computer-generated spotlight on the most productive workers.” [23]

Four in 10 Data Scientists Support Ethical Standard

Percentage of data scientists who agree …



Note: Based on survey of 144 data scientists at the American Statistical Association's Joint Statistical Meetings conference in Boston from Aug. 2–7, 2014.

Source: Survey data from Jeff Bertolucci, “Data Scientists Want Big Data Ethics Standards,” InformationWeek, Sept. 17, 2014, http://tinyurl.com/jwsnqpy

Almost half of data scientists surveyed at an American Statistical Association conference in August 2014 said Facebook's undisclosed 2012 psychological study of almost 700,000 users’ profiles was unethical. (Users were

not told the study was being conducted; it was disclosed later.) Forty-two percent of respondents said the big data industry should develop and implement an ethical standard for data collection.

The monitoring worked out well for Sullivan, who was recognized as a stellar employee and promoted to manager. Although the surveillance was legal, the article provoked angry comments on The Times' website from readers complaining that it was overly intrusive.

Sullivan's workday was scrutinized by NCR's Restaurant Guard, a program that monitors restaurant transactions in real time, using artificial intelligence to detect patterns of fraud and to spot performance bottlenecks. Using software that detects specified keywords, many employers monitor telephone calls and network traffic, including even emails sent from an employee's private email account. Some companies also employ video cameras to watch employees and geolocation tools to track employees with company cars or cellphones.

Internet and email monitoring is most prevalent, but 12 percent of businesses in a recent survey also acknowledge monitoring blogs and 10 percent track social networking sites to see what is being written about the company. [24]

The public's suspicions about Restaurant Guard's intrusiveness led Andrew McAfee, co-director of the Initiative on the Digital Economy at the Massachusetts Institute of Technology's Sloan School of Management, to write a Harvard Business Review column in defense of the software. He argued that it "doesn't engage in surveillance of employees' personal electronic communications, or any other activity they might reasonably consider private. Instead, it monitors their on-the-job performance, which is exactly one of the things that managers are supposed to do." [25] Other business professors and consultants cite specific reasons for employers to monitor employees.

Using software that detects specified keywords, many employers monitor telephone calls and emails sent from an employee's private email account. (Chris Ratcliffe/Bloomberg via Getty Images)

"Most of this monitoring is perfectly legal and even prudent in today's employment arena," wrote Ciocchetti of the University of Denver. "While employee monitoring remains a contentious issue, employers have good reasons for checking in on their employees' activities. Sexual or pornographic e-mails and Web pages, containing pictures or merely sexually explicit language, can form the basis for a harassment lawsuit. Excessive personal use of company broadband capacity or e-mail accounts will lead to decreased productivity, storage shortages and slower network operations. Failing to monitor is also likely to allow rogue employees to steal trade secrets or send out confidential information in violation of various federal and state laws." [26]

Nancy Flynn of the ePolicy Institute, an electronic policy consulting firm based in Columbus, Ohio, agrees. "In the United States, employers have a legal right to monitor all of the content and activities that take place on the organization computer system, accounts and devices," Flynn says. "So all employers as a best practice should take advantage of their legal right and monitor everything that is taking place on their computer systems."

Flynn also advises clients to monitor social media sites. "You want to see what people are saying," she says. She concedes, however, that monitoring employees' personal social media is "trickier." First, she notes that 17 states have laws preventing employers from asking for employee login information.

For employers in the other states, Flynn cautions against going on "fishing expeditions." She says, "You only want to do this if you have legitimate suspicion that, for example, confidential company information has been posted online or consumers' personal financial or health information has been exposed online."

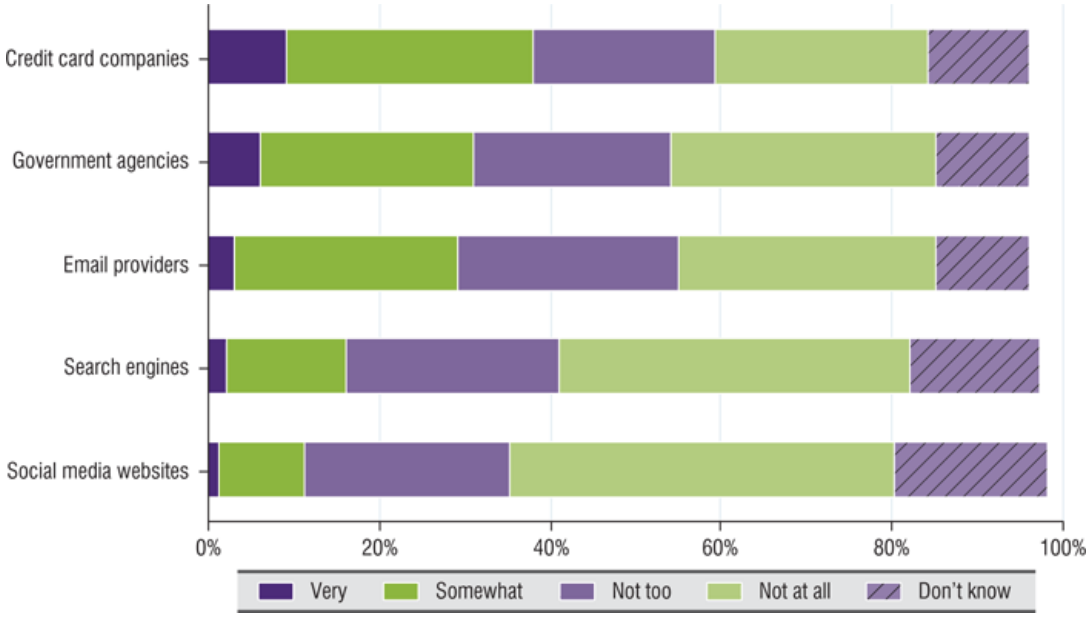
While most academics and privacy advocates are not against all monitoring, many say there should be legal limits that enforce ethical boundaries.

"The American legal system's effort to protect employee privacy is a patchwork of federal and state laws combined with the common law tort of intrusion upon seclusion," wrote Ciocchetti. "This regime is not properly equipped to defend against excessive invasions of privacy that come from increasingly sophisticated monitoring practices." [27]

"Most employees know that their employer has the ability to conduct surveillance but they have no idea how much surveillance is really happening or the circumstances under which it happens," says Lewis Maltby, president of the National Workrights Institute, a worker advocacy group based in Princeton, N.J. For example, Maltby notes that many employees think that their boss looks at their email or Internet traffic only when there's a reason to do so. "But that's not how it works," he says. "It's an open secret that IT techs read other employees' emails for fun. And many employers don't even have a paper policy against this."

Majority Doubt Companies, Agencies Will Protect Records

Percentage of adults who say records of their activities maintained by various types of organizations will remain private and secure, by confidence level



Notes: Based on online survey of 498 U.S. adults from Aug. 5–Sept. 2, 2014. Totals do not add to 100 percent because those who refused to respond are not shown.

Source: Mary Madden and Lee Rainie, "Americans' Attitudes About Privacy, Security and Surveillance," Pew Research Center, May 20, 2015, p. 7, http://tinyurl.com/j6lmk7 m

Nearly 70 percent of U.S. adults say they are "not too" or "not at all" confident that social media websites will keep their activity records private and secure, according to a summer 2015 Pew Research Center survey. Two-thirds say they are just as unsure about search engine companies protecting their activity records, and more than half say the same of government agencies and email providers.

Maltby says that while he thinks legislation is needed to protect worker privacy rights at work, adoption of best practices by companies is at least as important. "There are companies that do it right," he says. He cited one hotel chain that conducts monitoring, but only when a manager gets clearance from the chief privacy officer after demonstrating a specific need.

"We're not saying don't do it," Maltby says. "We're saying do it right."

Is software too open to abuse?

In 2000, Wells Fargo bank offered a "community calculator" to visitors to its website that purported to help homebuyers find the right place to live. To use the calculator, visitors were prompted to enter the ZIP code of their current residence, along with other data. The calculator used demographic data to determine the visitor's likely race and then steered whites to white neighborhoods and blacks to black neighborhoods. [28]

The company eventually dropped the calculator, after the Association of Community Organizations for Reform Now (ACORN), a now-defunct community activist group, filed a lawsuit. While it was impossible to tell what was going on under the hood of the calculator, ACORN was tipped off to the bias by the use in Wells Fargo documents of racial descriptions to categorize neighborhoods depicted as downtrodden. [29]

Whether deceptive code, unintended bugs or vulnerabilities, in most cases it's impossible for outsiders to know what actions software actually performs.

Because of the inherent opacity of software, some experts are calling for the widespread adoption of open-source software—software for which the underlying source code is made freely available for inspection and even modification by anyone. That, say open-source advocates, is the best way to deter companies from burying unrelated unannounced functionality in code. For their part, while several companies declined interviews on this issue, they have generally argued that their source code is a trade secret and essential to their competitiveness.

“Software has vulnerabilities in it, whether it's free or proprietary,” says Sandler of the Software Freedom Conservancy.

Open-source software, because it can be examined by outside programmers, is more resistant to bugs, vulnerabilities and deceptive code, advocates say. “Free and open software is better and safer over time,” Sandler says. “And if there is a problem, it can be fixed very quickly.”

Wasserman at Carnegie Mellon University agrees. “Transparency is a good thing,” he says. “The ability to see what is actually going on in any piece of software is beneficial.”

Others—especially software vendors—argue that open-source software often doesn't match the standards of proprietary software, particularly when it comes to security and new features.

“Security mechanisms must walk a careful balance between being open for review and being secret to protect specific information,” wrote Jim Allchin, group vice president for platforms at Microsoft Corp., in testimony during a 2002 court case. “It is generally a good practice not to disclose specifics of the implementation of a security mechanism. By analogy, a jewelry store might show off its safe to customers, with thick steel walls and complicated locks. However, the jewelry store would not post safety inspection schedules, fire alarm tests, or similar information relating to its safe.” [30]

Only one year after Allchin's testimony, anxious for sales in China and under pressure from the Chinese government, Microsoft agreed to disclose source code for its Windows operating system, but only to certain government clients, including the Chinese. [31]

Microsoft did not respond to interview requests for this report.

Some analysts note that proprietary software delivers one thing that open-source software does not—profit. “Proprietary software exists for one simple reason: as a means of enabling software as such to generate revenue,” wrote tech journalist John Carroll. And besides gratifying shareholders, profit can drive development of new features and products. “When software generates profit, it enables companies to grow, attracts investment (as investors prefer profitable companies as a place to put their money) and enables those companies to grow into tremendous sources of innovation and local employment,” Carroll wrote. [32]

Rather than pushing for the demise of proprietary software, some experts have proposed a compromise: Require disclosure of source code in return for software receiving patent protection. That would allow companies to keep their code proprietary and protected from competitors, but also would provide regulators an opportunity to detect deceptive code, thus deterring the practice.

According to Martin at George Washington, even if the disclosure was not made publicly available, it could deter patent applicants from including hidden functionality. “If we require them to disclose, then we could get them for lying about it in addition to whatever bad practices or unethical practices they were doing in the algorithm,” Martin says.

It would be more practical to amend current laws that prevent researchers from examining the inner workings of software, said Cardozo at the Electronic Frontier Foundation.

Cardozo notes that the 1998 Digital Millennium Copyright Act (DMCA), which governs digital intellectual property rights, makes it a crime to circumvent access control measures on digital devices.

“The DMCA prevents researchers from digging into code to see what it is actually doing,” Cardozo says. “The Copyright Office will enforce this and will allow companies to bring copyright infringement claims against, for instance, a researcher who wanted to dig into the Volkswagen engine control unit to see what it was doing.”

According to Section 1201 of the DMCA, researchers who examined the working of protected software would be violating the law even if they did not appropriate or change the software.

Cardozo argues for reform or outright repeal of Section 1201. “That would rebalance the table and allow consumers to open the hood and see what is going on in products they already own,” he says.

According to Cardozo, automakers are lobbying against such changes. “They’re pushing back pretty hard on the grounds that allowing people to look under the hood of their own cars poses a safety and environmental risk,” he says. “This, despite the fact that Volkswagen's behavior shows that not allowing people to look under their hoods actually posed a risk.”

In written comments to the U.S. Copyright Office, arguing against a proposal that would partially exempt automobiles from Section 1201 protections, General Motors contended, “While proponents such as Electronic Frontier Foundation characterize the exemption as merely allowing the vehicle owners to ‘tinker’ with their vehicles ‘in a decades-old tradition of mechanical curiosity and self-reliance,’ if granted, the proposed exemption could introduce safety and security issues as well as facilitate violation of various laws designed specifically to regulate the modern car, including emissions, fuel economy, and vehicle safety regulations.” [33]

Background

Early Issues

Each advance in technology presents new opportunities and new challenges for company interactions with the public, with regulators and with employees.

When the nascent nation's postal service was established in 1775, for example, no law barred anyone from opening mail in transit. And while many considered opening mail to be unethical, it was routinely done until Congress in 1782 made opening mail in transit illegal. [34]

"While the Constitution's Fourth Amendment codified the heightened privacy protection afforded to people in their homes or on their persons (previously principles of British common law), it took another century of technological challenges to expand the concept of privacy rights into more abstract spaces, including the electronic," according to a 2014 report from the President's Council of Advisers on Science and Technology. "The invention of the telegraph and, later, telephone created new tensions that were slow to be resolved. A bill to protect the privacy of telegrams, introduced in Congress in 1880, was never passed." [35]

Eastman Kodak's introduction of inexpensive portable cameras gave rise to the first push for a general privacy law. (George Rose/Getty Images)

The introduction of inexpensive portable cameras—marketed to the masses after the founding in 1888 of what became the Eastman Kodak Co.—gave rise to the first real push for a general privacy law. In their seminal 1890 article, lawyers Samuel Warren and Louis Brandeis, a future Supreme Court justice, wrote, "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.' For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons." [36]

As the President's Council of Advisers on Science and Technology noted, it took another 75 years for the Supreme Court to determine—in Griswold v. Connecticut (1965)—that citizens have a constitutionally protected right to privacy. The advisory council cited several specific meanings of "privacy" that have subsequently been derived from the ruling, including the individual's right to keep secrets or seek seclusion and the ability to control access by others to personal information after it leaves one's exclusive possession.

Only two years later, however, the Supreme Court specifically established in Katz v. United States that a conversation is protected from unreasonable search and seizure under the Fourth Amendment only if it is made with a "reasonable expectation of privacy." According to Reynolds of Strayer University, subsequent decisions soon made it clear that employees have no reasonable expectation of privacy in most circumstances at work. "The Fourth Amendment cannot be used to limit how a private employer treats its employees," wrote Reynolds. [37]

Big Data

Arguably, the first major private-sector big data effort was that of consumer credit reporting agencies, which first appeared in the 1950s. Throughout the 1960s, credit reporting companies were industry specific and community-centric. "As such, bank-, retailer-, or finance company-sponsored 'bureaus' did not share loan or inquiry information with each other," wrote Mark Furletti, an analyst at the Federal Reserve Bank of Philadelphia. "This kept banks from knowing about loans or inquiries made by finance companies or retailers and vice versa. The situation limited any creditor's ability to understand a potential customer's entire debt situation." [38] However, there was no assurance that the data collected was accurate, and once one company shared data with another, the errors could be very difficult for consumers to learn about, much less correct.

As credit-reporting companies began to share data, Congress responded with the Fair Credit Reporting Act (FCRA), aimed at ensuring the accuracy and fairness of the data being collected. The act requires that consumers have an opportunity to view, correct and challenge the contents and uses of their credit reports. "The industry stopped reporting things like marriages, promotions, and arrests and focused its efforts on reporting verifiable credit-related information," Furletti said. "This included both positive information, such as a consumer's ability to consistently pay her bills on time, as well as negative information, such as defaults and delinquencies." [39]

Congress followed up in 1996 with another major privacy-protection law, the Health Insurance Portability and Accountability Act (HIPAA), which regulates companies' management of consumers' health-related data.

In 1997, the Federal Trade Commission (FTC)—the primary agency responsible for enforcing the credit-reporting law—turned its attention

to examining the activities of data brokers, companies that collect data from a variety of public and private sources for analysis. In response to an FTC-sponsored workshop, data brokers that year voluntarily formed the Individual Reference Services Group to provide self-regulation for the industry.

Self-regulation did not work, according to a 2014 FTC report. What's more, in the wake of that "short-lived" effort, the report said, "data broker practices have grown dramatically, in both breadth and depth, as data brokers have expanded their ability to collect information from a greater number of sources, including from consumers' online activities; analyze it through new algorithms and emerging business models; and store the information indefinitely due to reduced storage costs. Despite the Commission's past recommendations, lack of transparency and choice remain a significant source of concern about this industry." [40]

The FCRA and HIPAA, though limited in scope, remain the primary regulatory authority over private-sector uses of big data. From 2002 to 2014, the FTC initiated more than 50 actions against companies that it alleged engaged in unfair or deceptive practices involving consumer data, with many of the cases resulting in multimillion-dollar fines. [41]

Electronic Privacy

As new and more powerful technologies—computers, email, the Internet, cellphones—delivered more powerful communications and data-gathering tools to companies and consumers alike, they also created new opportunities for invasions of privacy by governments, companies and individuals. The first major legislation specifically relating to abuses involving computer and other digital technologies in the private sector was the Electronic Communications Privacy Act (ECPA) of 1986. Fundamentally, the law extended existing regulations governing wiretaps of telephone calls to include transmissions of electronic data by computers. The ECPA also prohibited some access to stored electronic communications.

While the restrictions of the ECPA apply to private-sector companies just as they do to government agencies, as a result of two statutory exemptions, they do not inhibit employers' actions with respect to employees at the workplace or using company equipment. The first exemption allows "a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose or use that communication." In short, if the employer provides the service, interception is allowed. According to some experts, however, it is not clear if that exemption holds up if the employer contracts with an outside service provider. [42]

The second exemption is if the employer obtains the implied or express consent of employees. "If an employee has knowledge of the employer's policy and he or she continues to use the system anyway, this will likely fall under the consent exception. In practice, moreover, many employers routinely require employees to acknowledge—if not explicitly sign away any residual rights—that the employer may monitor computer usage including internet and email access," according to course materials at the Berkman Center for Internet and Society, a research program at Harvard Law School. [43]

Critics complain that the electronic privacy law not only is too limited in scope but also is seriously outdated. "The ECPA was intended to extend privacy protection from wire communications such as telephone calls to electronic communications such as e-mails and text messages," wrote Ciocchetti of the University of Denver. "The problem is that contemporary technology has advanced tremendously since 1986, and the ECPA is not equipped to keep pace." [44]

Specifically, the act protects messages only while they are in transmission, and once they are stored the wiretap protection provisions do not apply. "This is a major distinction because the vast majority of electronic communications are only 'in transmission' for mere seconds before arriving at their destination," Ciocchetti said. [45]

Finally, Ciocchetti noted that no federal law—and only two state laws—require that notice be provided to employees prior to monitoring. What's more, he added, "for the most part, private employers must intrude into very private places—such as restrooms or locker rooms—in order to face liability for intrusion upon seclusion." [46]

Regulating Software

When software—the instructions that direct a computer to perform specific operations—was introduced in the 1940s, it was not considered eligible for either copyright protection or patent protection. That was a major concern for companies that were investing money in developing software and wanted to protect that investment. Software companies responded in two ways: first, by keeping the source code for the software secret so others would find it difficult to reproduce; second, by lobbying for legislation protecting software.

"In the 1960s and early 1970s, computer programs enjoyed very limited intellectual property protection," wrote Robert M. Hunt, an economist at the Federal Reserve Bank of Philadelphia. "And it was widely believed that patent protection for computer programs was unavailable. This impression was bolstered by a 1972 Supreme Court decision (Gottschalk v. Benson) involving an application to patent a computer program that translated decimal numbers into binary numbers. The court concluded the program was a mathematical algorithm, which, like laws of nature or an abstract idea, does not fall into one of the categories of patentable subject matter." [47]

It wasn't until 1980 that Congress amended the Copyright Act to explicitly cover software. But by then it was already clear to software manufacturers that copyright protection was of little use to them, because all it protected was the specific expression of the coding. There was nothing in copyright law to prevent competitors from examining the code and replicating its functionality.

In 1994, software companies received help from the U.S. Court of Appeals, Federal Circuit, which ruled definitively that a computer program was patentable. And unlike copyrights, patents protected not just the instance of the invention but also the idea of its functionality. The Patent Office had rejected the patent application by three engineers who had created a program to modify the output of an oscilloscope on the ground that it lacked any physical transformation of matter. The court, however, ruled that the software was in essence a machine and was, thus, patentable. [48]

In 1998, the Digital Millennium Copyright Act made it illegal to evade copy protection measures.

In 2014, the Obama administration released a report from a task force that included two Cabinet members and several other senior officials about the ways in which government could enhance the accountability of big data. A year later, the task force issued a second report calling for an array of measures including adoption of a White House-proposed Consumer Privacy Bill of Rights and amendment of the Electronic Communications Privacy Act to ensure the standard of protection for online content is consistent with that afforded in the physical world.

“The declining cost of data collection, storage, and processing, coupled with new sources of data from sensors, cameras, and geospatial technologies, means that we live in a world where data collection is nearly ubiquitous, where data retention can be functionally permanent, and where data analysis is increasingly conducted in speeds approaching real time,” noted the task force's 2015 report. “While there are promising technological means to better protect privacy in a big data world, the report's authors concluded these methods are far from perfect, and technology alone cannot protect privacy absent strong social norms and a responsive policy and legal framework.” [49]

Current Situation

Best Practices

The recent Volkswagen scandal and strings of major data breaches have given rise to calls from advocacy groups, professional organizations and academicians to implement measures to encourage best practices within companies.

Many experts say that expanded training in ethics is needed both in companies and in business schools. Flynn of the ePolicy Institute says companies will be facing increasing ethical quandaries with respect to their own employees.

“I do think that given the fact that we are now looking at a young workforce, coming into business—people who have grown up with electronic devices, and particularly mobile devices—organizations are going to start to face more and more ethical challenges and resistance from employees,” Flynn says. “When employers try to impose restrictions on them, they’re going to meet more resistance than they have met in the past. So I think employers are going to be finding themselves increasingly in a position … where they’re wrangling more and more with ethical issues.”

While noting that almost all engineering programs have mandatory ethics classes, Martin at George Washington says the same is not true at business schools. “We’re not very good at it,” she says. As a faculty member, Martin has reviewed dozens of course proposals and has noted that they rarely focus on ethical issues. “For one of my papers I went out and looked at 15 proposals,” she recalls. “I figured there must be one program in big data analytics that has an ethics requirement. I looked through the curricula and there was no ethics requirement.”

Penny Duquenoy: “Technology people don't tend to talk in terms of ethics.”

Finally, some experts argue that ethical training isn't just about “doing the right thing.” Over the long haul, it's also the smart thing. “Being ethical is good for business, at least for a sustainable business,” says Duquenoy at Middlesex University in London, who specializes in the ethical implications of information technology.

Despite Duquenoy's conviction that ethical behavior is good for business, she says it can often be difficult to communicate that in the workplace. “Technology people don't tend to talk in terms of ethics,” she says. In the end, according to Duquenoy, the strongest arguments aren't about ethics as much as about potential consequences. “It comes down to a risk analysis and a cost-benefit, and whether doing something is worth the risk,” she says.

Current Legislation

Despite calls from the White House, Congress has shown little interest in regulating companies’ use of digital technologies. The sole piece of legislation introduced in the current Congress that is related to private-sector uses of technology directly affecting consumers or employees is the Data Broker Accountability and Transparency Act of 2015 (S. 668) introduced by Sen. Ed Markey, D-Mass. [50]

The bill, which was sent to committee in March 2015, would require any commercial entity that collects, assembles or maintains personal information to establish procedures to ensure the accuracy of that

information and to provide individuals with a cost-free means of reviewing their personal data. The bill also calls for procedures to allow consumers to dispute data and for an “opt-out” provision that would allow individuals to prevent personal data from being collected and used.

While consumer groups and privacy advocates have generally praised the bill, critics complain that its scope is far too broad. “Time and again, Congress has found that access and correction to consumer data are necessary only when the information is used for eligibility purposes, and marketing is not an eligibility purpose,” said Peggy Hudson, the Direct Marketing Association's senior vice president of government affairs, in response to the introduction of almost identical legislation in 2014. “Imposing an access and correction regime on marketing data is not necessary to protect consumer privacy and doing so would make it harder for companies to keep data secure at a time when consumers are more concerned about identity theft than ever before.” [51]

The DMA, an industry advocacy organization, declined interview requests for this report.

As of early 2016, the bill had just three co-sponsors—all of them Democrats—and most analysts gave it almost no chance of being approved. GovTrack, a nonpartisan company that monitors and analyzes legislation, gave the bill only a 4 percent chance of passage. [52]

Consumer Bill of Rights Act

The other major proposed legislation, which has not yet been introduced in Congress, is the Consumer Bill of Rights Act. The Obama administration followed up on its 2012 report calling for a Consumer Bill of Rights with draft legislation in February 2015. [53]

Among its provisions, the draft bill would provide:

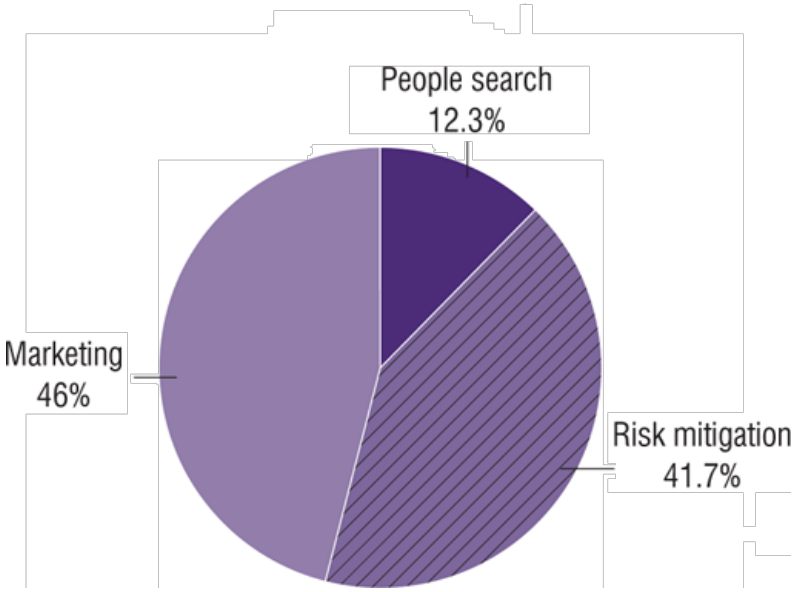
- **Individual control**: Give consumers the right to exercise control over what personal data is collected and how it is used.
- **Transparency**: Require data collectors to make privacy and security practices accessible and understandable.
- **Respect for context**: Require companies to collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- **Security**: Require companies to secure personal data.
- **Access and accuracy**: Give consumers the right to access and correct personal data.

While generally welcomed by consumer groups and privacy advocates as a first step, the proposal has drawn criticism from all sides.

“The administration's concrete legislative proposal is an incredibly important step,” noted the Center for Democracy & Technology in its analysis of the bill. “A number of elements need to be improved if this bill is going to offer consumers comprehensive protection. As it is, there are too many loopholes, and enforcement is noticeably lacking.” [54]

Data Brokers Rely on Marketing Revenue

Percentage of revenue at data brokers, by product type, 2012



Note: Based on federal study of data collection practices by a sample of nine data brokers in 2012. Percentages have been calculated from revenue total in $U.S.

Source: "Data Brokers: A Call for Transparency and Accountability," Federal Trade Commission, May 2014, p. 23, http://tinyurl.com/mwury6w

Nearly half the annual revenue at a sample of nine data brokers came from selling data for marketing purposes, according to a Federal Trade Commission study. Risk mitigation—including identity verification and fraud detection—was the second-largest revenue generator, (42 percent), followed by people search products (12 percent), such as consumer directories and search tools.

The center particularly dislikes that privacy fines would be calculated not by the number of individuals affected by a violation but by the number of days that a violation persisted. "Thus, if a multibillion-dollar company decided to sell millions of records in one day in violation of its promises, under this bill it would face a maximum fine of $35,000—an incredibly perverse result," the report said.

Industry groups were even more critical of the proposal, warning that its provisions are both costly and unnecessary. Gary Shapiro, president of the Consumer Electronics Association, said that such legislation "could hurt American innovation and choke off potentially useful services and products." [55]

Likewise, a representative of the Internet Association, an industry group that represents Internet companies, including Google and Facebook, said in early 2015 that privacy rules should be "finely tailored to address specific harms," and the proposal in contrast cast "a needlessly imprecise net" that could "create a drag on our economy." [56]

Looking Ahead

"New Generation of Nuance"

Technology has fundamentally changed the nature and extent of the ethical challenges facing businesses, experts say.

"What we are seeing now is a new generation of nuance as regards accountability and responsibility," says the University of Miami's Goodman. And he is not optimistic about preventing such abuses in the near future. "The idea that software can be used daily to deceive people, or government regulators, is a bit of a wake-up call," he says. Given that technology is inherently opaque, Goodman says, trusted entities must serve as watchdogs. "I'm sentimental enough to hope that that might be journalists, but I'm despairing of journalism these days, too," he says.

Ultimately, Goodman says, people have to take personal responsibility for their behaviors. Referring again to the Volkswagen scandal, he says, "It goes straight to the people who wrote the code and the people who ordered it to be used. These are human beings who intentionally used the tools of their trade to deceive."

Martin at George Washington suggests that broadened whistleblower protections and requirements for disclosure of source code may

help encourage ethical behavior. “If we require them to disclose [code in a patent] application,” she says, “then we could get them for lying about it in addition to whatever bad practices or unethical practices they were doing in the algorithm.”

Otherwise, “I don't know how you’d regulate it,” Martin says. “I really don’t. People with technology just figure out a way to not fall within the scope of the regulation.”

Martin says that such measures are unlikely to get through the currently divided government in the United States. As a result, she says, she expects change will only come “either through public shaming or through lawsuits.”

Goodman agrees. “It's cases like Volkswagen … when people realize that they are not on a level playing field with the businesses that have rigged these games,” he says. “I am hoping that the Volkswagen scandal kicks a bunch of people in the butt.”

“I hate to say it, but what we are going to need is more failures,” echoes Sandler at the Software Freedom Conservancy. She says that ensuring ethical use of technology will require a change in technology cultural values. “We need a culture among the engineers to understand that there is that responsibility to speak out,” she says, where whistleblowers are accepted. “I think we need a culture of understanding the social implications around our technology.”

The stakes are high, warned law professor Neil M. Richards and Jonathan H. King, vice president at CenturyLink Technology Solutions, a nationwide communications provider headquartered in Monroe, La. “We are building a new digital society, and the values we build or fail to build into our new digital structures will define us,” they wrote. “Critically, if we fail to balance the human values that we care about, like privacy, confidentiality, transparency, identity, and free choice, with the compelling uses of big data, our big data society risks abandoning these values for the sake of innovation and expediency.” [57]

About the Author

Patrick Marshall is a freelance writer in Seattle who covers public policy and technology issues. He is a technology columnist for The Seattle Times and Government Computer News. He holds a B.A. in anthropology from the University of California, Santa Cruz, and a master's degree in international studies from the Fletcher School of Law and Diplomacy, a program of Harvard and Tufts universities.

Chronology

1700s–1900s	**New technologies challenge privacy.**
1782	After complaints about the security of mail in the nation's new postal service, which was established in 1775, Continental Congress passes legislation making the opening of mail in transit illegal.
1890	Shortly after the introduction of the inexpensive and portable Kodak camera, lawyers Samuel Warren and Louis Brandeis, a future Supreme Court justice, warn that “instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’ ”
1950s–1970s	**Consumer databases attract regulation.**
1965	In Griswold v. Connecticut, the Supreme Court rules that citizens have a constitutionally protected right to privacy.
1967	The Supreme Court holds in Katz v. United States that a conversation is only protected from unreasonable search and seizure under the Fourth Amendment if it is made with a “reasonable expectation of privacy.” Subsequent decisions make it clear that employees have no reasonable expectation of privacy in most circumstances at work.
1970	Congress passes the Fair Credit Reporting Act to promote the accuracy, fairness and privacy of consumer information contained in the files of consumer reporting agencies. The act regulates the collection, dissemination and use of consumer information, including consumer credit information.
1972	The Supreme Court decides in Gottschalk v. Benson that computer programs cannot be patented, ruling that mathematical algorithms are abstract ideas like laws of nature.
1980s–1990s	**Legislators tackle computer technology.**
1980	Congress amends the Copyright Act to explicitly cover software, but manufacturers find it of little use because it doesn't protect others from copying the program's functionality.

1986	The Electronic Communications Privacy Act extends existing regulations governing wiretaps of telephone calls to include transmissions of electronic data by computers.
1994	Federal courts hold that computer programs can be patented.
1995	The European Union passes the Data Protection Directive, which puts clear limits on the collection and storage of personal data by companies.
1997	The Federal Trade Commission (FTC) examines the activities of data brokers—companies that collect and analyze consumer data. In response to an FTC-sponsored workshop, data brokers voluntarily form the Individual Reference Services Group to provide self-regulation for the industry. Self-regulation was short-lived.
1998	The Digital Millennium Copyright Act makes it illegal to attempt to circumvent protection schemes in software and digital devices. Critics argue that the act allows bad actors to hide unethical or illegal code.… The Environmental Protection Agency announces settlements totaling in the hundreds of millions of dollars with carmakers Honda and Ford resulting from the companies' use of "defeat devices" to get around emissions control systems.
2000s–Present	**Calls for regulation of technologies increase.**
2002	The European Union (EU) adopts the e-Privacy Directive, which extends the protections of the Data Protection Directive to telecommunications, specifically all publicly available telecommunications networks in the EU.
2009	Heartland, a Princeton, N.J.-based payment processor, announces that cybercriminals had penetrated its databases and acquired information on approximately 130 million credit and debit cards.
2012	The Obama administration calls for a Consumer Privacy Bill of Rights that will ensure consumer control over personal data and how it is used; it also calls upon private-sector companies to adopt enforceable codes of conduct.
2014	The Federal Trade Commission urges legislation that would, among other things, require data brokers to give consumers access to their data. The report also recommends mandatory "opt-outs" that would give consumers to right to prevent their data from being collected.
2015	Volkswagen publicly admits that it had installed software in 11 million diesel automobiles designed to deceive emissions tests. (August) The incident renews calls for amending the Digital Millennium Copyright Act to allow regulators and researchers to examine software.… The European Court of Justice rules invalid an international pact that governed the movement of data—such as individuals' Internet search histories and social media data—between the EU and the United States. (October) The court concludes that "the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities of the data transferred to that country."

Resources

Bibliography

Books

Bamberger, Kenneth A., and Deirdre K. Mulligan, "Privacy on the Ground: Driving Corporate Behavior in the United States and Europe," MIT Press, 2015. A University of California, Berkeley, law professor (Bamberger) and a professor at Berkeley's School of Information (Mulligan) explain the regulations governing corporate use of consumer data in five countries, including the United States, and how those regulations shape company behavior.

Howard, Philip N., "Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up," Yale University Press, 2015. A communications professor at the University of Washington outlines the challenges to come in the age of the Internet of Things and suggests measures to ease the way.

Schneier, Bruce, "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World," W.W. Norton & Co., 2015. A security expert explores, and explains, the reach and power of surveillance tools that corporations and governments are using.

Articles

Barocas, Solon, and Andrew D. Selbst, "Big Data's Disparate Impact," California Law Review, 2016, http://tinyurl.com/j6ovlkc. A technologist and a lawyer team up to examine the ways in which algorithms used in big data analytics can discriminate against groups of people.

Hunt, Robert M., "You Can Patent That? Are Patents on Computer Programs and Business Methods Good for the New Economy?" Business Review, Federal Reserve Bank of Philadelphia, First Quarter 2001, http://tinyurl.com/hzao6ga. A Federal Reserve Bank economist offers a history of patent protection for software and questions whether the current system is a good one.

Richards, Neil M., and Jonathan H. King, "Big Data Ethics," Wake Forest Law Review, May 19, 2014, http://tinyurl.com/hz33hlm. A law professor (Richards) and a technology company executive (King) examine the ethical issues confronting those performing big data analytics.

Reports and Studies

"Big Data and Privacy: A Technological Perspective," President's Council of Advisers on Science and Technology, May 2014, http://tinyurl.com/p92vpo5. A report by a White House technology panel recommends that regulators focus on the uses of big data by companies rather than on collection and storage.

"Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," White House, Feb. 23, 2012, http://tinyurl.com/judzdv9. A White House report calls for legislation creating a "Consumer Bill of Rights" that would restrict what companies can do with consumer data.

"Data Brokers: A Call for Transparency and Accountability," Federal Trade Commission, May 2014, http://tinyurl.com/mwury6w. This 110-page report from the federal agency that oversees consumer protection offers a thorough examination of the data broker industry and finds it lacking in transparency.

"The Latest on Workplace Monitoring and Surveillance," American Management Association, Nov. 17, 2014, http://tinyurl.com/yjb4q4a. Corporate training group offers a wealth of up-to-date survey data on the surveillance and monitoring practices of U.S. companies.

"A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes," Senate Committee on Commerce, Science and Transportation, Office of Oversight and Investigations Majority Staff, Dec. 18, 2013, http://tinyurl.com/h5gvfhw. A Senate report examines the growth of the multibillion-dollar data broker industry and finds that it operates hidden from consumer view.

Ciocchetti, Corey A., "The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring," May 29, 2010, http://tinyurl.com/jfy8enl. A professor of ethics and legal studies at the University of Denver's Daniels College of Business says the American legal system has failed to keep up with changes in monitoring technologies.

Furletti, Mark J., "An Overview and History of Credit Reporting," Discussion Paper, Federal Reserve Bank of Philadelphia, June 2002, http://tinyurl.com/gnnlr7g. An analyst at the Federal Reserve Bank of Philadelphia provides a concise and interesting history of the development of consumer credit databases and reporting services.

The Next Step

Big Data

Clover, Charles, "China: When big data meets big brother," Financial Times, Jan. 19, 2016, http://tinyurl.com/ztcmzg2. The Chinese government has licensed eight companies to collect Web users' data and develop so-called "social credit" ratings that affect eligibility for activities ranging from travel to pet adoption, a practice that some have deemed mass surveillance.

Darrow, Barb, "Coming Soon: Ethics Training for Data Scientists," Fortune, Dec. 4, 2015, http://tinyurl.com/zdw4tg5. All university data science programs will add classes in 2016 on the human implications of mass data collection, a principal data researcher for Microsoft predicts.

Green, Chloe, "By 2018 big data will be responsible for half of ethics violations in business – study," Information Age, Oct. 7, 2015, http://tinyurl.com/gl2rg2y. Big data collection will cause up to half of all business ethics violations by 2018, although companies can cautiously invest in advanced analytics and implement clear strategies for their use to reduce future violations, according to a U.S. market research firm.

Employee Monitoring

Melendez, Steven, "The Office Is Watching You," Fast Company, May 22, 2015, http://tinyurl.com/ooor6en. Technology start-ups are developing software that other companies can use to track employee time spent in meetings and track behavior and workplace engagement levels.

Shockman, Elizabeth, "Gamifying the workplace: is it ethical?" Science Friday, Public Radio International, Sept. 5, 2015, http://tinyurl.com/h4wpl4e. More companies have introduced software in offices in recent years that track employee health habits to optimize performance, though some say such technologies can be disruptive and disregard the personal interests of employees.

Son, Hugh, “JPMorgan Algorithm Knows You’re a Rogue Employee Before You Do,” Bloomberg Business, April 8, 2015, http://tinyurl.com/qy5e6qw. Financial services firm JPMorgan Chase will introduce an employee-surveillance program in 2016 that uses algorithms to track whether workers follow trading rules and complete compliance courses, among other criteria, to reduce legal risks.

Europe

Ashford, Warwick, “EU privacy watchdog to set up ethics advisory group,” Computer Weekly, Jan. 6, 2016, http://tinyurl.com/j5wqg6t. The European Union's independent supervisory data-protection body plans to form an ethics advisory group that will recommend ways for the EU to use new technologies while protecting personal privacy.

Scott, Mark, and Natasha Singer, “How Europe Protects Your Online Data Differently Than the U.S.,” The New York Times, Jan. 31, 2016, http://tinyurl.com/zzdtc2p. The EU grants Web users more data-related protections than the United States, including the rights to request that search engines remove links with personal information from results and that companies share personal data they have collected and how they are using it.

Wagner, Kurt, and Mark Bergen, “Europe's 'safe Harbor’ Ruling: A Headache for Tech Giants, but a Blow to the Little Guys,” re/code, Oct. 6, 2016, http://tinyurl.com/jcnwx9m. A 2015 European Court of Justice ruling, which invalidated an agreement that permitted American companies to transmit data gathered in Europe to the United States, will likely mostly harm small- and medium-sized companies that lack other data-collection arrangements with EU nations.

Hiring Discrimination

Lam, Bourree, “For More Workplace Diversity, Should Algorithms Make Hiring Decisions?” The Atlantic, June 22, 2015, http://tinyurl.com/oumx8aw. A software company that develops algorithms that can analyze job applicants’ behavioral data, predict their performance and compare it to that of top employees claims companies using its software would hire 26 percent more blacks and Hispanics on average.

Noguchi, Yuki, “How Startups Are Using Tech To Try And Fight Workplace Bias,” NPR, Sept. 1, 2015, http://tinyurl.com/ofpwnk6. Some software start-ups have developed technology that mitigates racial or gender bias by playing down résumés in favor of skill-based tests, and others have created training methods for managers that identify their hidden biases in evaluations.

Pepitone, Julianne, “Can Résumé-Reviewing Software Be As Biased As Human Hiring Managers?” NBC News, Aug. 17, 2015, http://tinyurl.com/zrpkxvs. Computer science researchers from the Universities of Arizona and Utah and Haverford College developed a test that they say detects hidden bias in supposedly gender- and race-blind hiring software.

Organizations

Center for Democracy and Technology
1634 I St., N.W., #1100, Washington, DC 20006
202-637-9800
cdt.org
Advocates laws, corporate policies and technology tools that protect the privacy of Internet users.

Direct Marketing Association
1333 Broadway, Suite #300, New York, NY 10018
212-768-7277
thedma.org
Industry organization that represents the interests of marketing companies and data brokers.

Electronic Frontier Foundation
815 Eddy St., San Francisco, CA 94109
415-436-9333
eff.org
Focuses on defending civil liberties in the digital world and lobbies for legislation at state and federal levels.

Electronic Privacy Information Center
1718 Connecticut Ave., N.W., Suite 200, Washington, DC 20009
202-483-1140
epic.org
Research center focused on technology-related privacy and civil liberties issues; also lobbies for privacy legislation.

The ePolicy Institute
2300 Walhaven Court, Columbus, Ohio 43220

614-451-3200
epolicyinstitute.com
Consulting group that offers seminars and webinars to clients seeking to minimize electronic risks, maximize compliance and manage employees' online use and content.

Federal Trade Commission
600 Pennsylvania Ave., N.W., Washington, DC 20580
202-326-2222
ftc.gov
Agency charged with preventing business practices that are anti-competitive or are deceptive or unfair to consumers; also holds workshops, makes legislative recommendations and conducts enforcement actions.

National Society of Professional Engineers
1420 King St., Alexandria, VA 22314
888-285-6773
nspe.org
Professional society that provides education and training, and advocates for measures aimed at protecting engineers and the public from unqualified practitioners.

National Workrights Institute
128 Stone Cliff Road, Princeton, NJ 08540
609-683-0313
workrights.us
Nonprofit spinoff from the American Civil Liberties Union that is focused on protecting human rights in the workplace.

Open Source Initiative
855 El Camino Real, Suite 13A, #270, Palo Alto, CA 94301
opensource.org
Educational and advocacy group that backs adoption of nonproprietary software; also serves as a licensing body for Open-Source Definition compliant software.

Notes

[1] Danielle Ivory and Keith Bradsher, "Regulators Investigating 2nd VW Computer Program on Emissions," The New York Times, Oct. 8, 2015, http://tinyurl.com/oqbl2ab.

[2] Jack Ewing, "Volkswagen, Hit by Emissions Scandal, Posts Its First Loss in Years," The New York Times, Oct. 28, 2015, http://tinyurl.com/ptqgr2c.

[3] Karl Russell et al., "How Volkswagen Got Away With Diesel Deception," The New York Times, Jan. 5, 2016, http://tinyurl.com/h697u97.

[4] James Temperton, "AVG can sell your browsing and search history to advertisers," Wired UK, Sept. 18, 2015, http://tinyurl.com/oat9j68.

[5] Corey Ciocchetti, "The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring," May 29, 2010, available at SSRN, http://tinyurl.com/jfy8enl.

[6] "The Latest on Workplace Monitoring and Surveillance," American Management Association, Nov. 17, 2014, http://tinyurl.com/yjb4q4a.

[7] Marc Rotenberg, "Comments of the Electronic Privacy Information Center to the Office of Science and Technology Policy Request for Information: Big Data and the Future of Privacy," Electronic Privacy Information Center, April 4, 2014, http://tinyurl.com/hbo2xvx.

[8] Kashmir Hill, "How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did," Forbes, Feb. 16, 2012, http://tinyurl.com/hp97tbj.

[9] "Big Data in Private Sector and Public Sector Surveillance," Electronic Frontier Foundation, 2014, http://tinyurl.com/hm2j37f.

[10] "Gartner Says, By 2018, Half of Business Ethics Violations Will Occur Through Improper Use of Big Data Analytics," news release, Gartner Inc., Oct. 7, 2015, http://tinyurl.com/hyxkypl.

[11] "2012 Institute Initiatives," Business Roundtable Institute for Corporate Ethics, undated, accessed Jan. 20, 2016, http://tinyurl.com/hdvrj73.

[12] George W. Reynolds, "Ethics in Information Technology," 2015, p. 12.

[13] For background, see Chuck McCutcheon, “Whistleblowers,” CQ Researcher, Jan. 31, 2014, http://tinyurl.com/hno4xsl.

[14] “Big Data & Analytics,” IDC, undated, accessed Jan. 20, 2016, http://tinyurl.com/z8o2fa8.

[15] “Data Brokers: A Call for Transparency and Accountability,” Federal Trade Commission, May 2014, http://tinyurl.com/mwury6w.

[16] Neil M. Richards and Jonathan H. King, “Big Data Ethics,” Wake Forest Law Review, May 19, 2014, p. 393, http://tinyurl.com/hz33hlm.

[17] “A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes,” Committee on Commerce, Science and Transportation staff report, Dec. 18, 2013, http://tinyurl.com/zdqh2lk.

[18] Rotenberg, op. cit.

[19] Kate Tummarello, “Rockefeller: ‘Data brokers’ worse than NSA spying,” The Hill, Dec. 18, 2013, http://tinyurl.com/ltry4zu.

[20] “A Review of the Data Broker Industry,” op. cit.

[21] Testimony of Tony Hadley before the Senate Committee on Commerce, Science and Transportation, Dec. 18, 2013, http://tinyurl.com/jyz9deb.

[22] Testimony of Jerry Cerasale before the Senate Committee on Commerce, Science and Transportation, Dec. 18, 2013, http://tinyurl.com/glgg6se.

[23] Steve Lohr, “Unblinking Eyes Track Employees,” The New York Times, June 21, 2014, http://tinyurl.com/n5zpsjs.

[24] “The Latest on Workplace Monitoring and Surveillance,”op. cit.

[25] Andrew McAfee, “In Praise of Electronically Monitoring Employees,” Harvard Business Review, Oct. 24, 2013, http://tinyurl.com/hbzwux9.

[26] Ciocchetti, op. cit.

[27] Ibid.

[28] Bruce Schneier, “Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World,” 2015, p. 109.

[29] “Lawsuit accuses Wells Fargo of using Net to discriminate,” The Associated Press, CNET, Sept. 6, 2002, http://tinyurl.com/zgljzk5.

[30] Written testimony of Jim Allchin, State of New York v. Microsoft Corp., U.S. District Court, May 3, 2002, http://tinyurl.com/j7f6c7j.

[31] Stephen Shankland, “Governments to see Windows code,” CNET, Jan. 30, 2003, http://tinyurl.com/zo53s8v.

[32] John Carroll, “Proprietary software: A defence,” ZDNet, Dec. 16, 2003, http://tinyurl.com/hhkpbl6.

[33] Comments of General Motors LLC before the U.S. Copyright Office, March 27, 2015, http://tinyurl.com/hntwwzu.

[34] “Big Data and Privacy: A Technological Perspective,” President's Council of Advisers on Science and Technology, May 2014, p. 3, http://tinyurl.com/p92vpo5.

[35] Ibid.

[36] Samuel D. Warren and Louis D. Brandeis, “The Right to Privacy,” Harvard Law Review, Dec. 15, 1890, http://tinyurl.com/nzkpn8t.

[37] Reynolds, op. cit., p. 156.

[38] Mark J. Furletti, “An Overview and History of Credit Reporting,” discussion paper, Federal Reserve Bank of Philadelphia, June 2002, http://tinyurl.com/gnnlr7g.

[39] Ibid.

[40] “Data Brokers: A Call for Transparency and Accountability,” op. cit.

[41] “Federal Trade Commission 2014 Privacy and Data Security Update,” Federal Trade Commission, 2014, http://tinyurl.com/h32cyxz.

[42] “Privacy in Cyberspace, Module 3; Introduction: Privacy in the Workplace,” Berkman Center for Internet and Society Harvard Law School, undated, accessed Jan. 21, 2016, http://tinyurl.com/7jvco6f.

[43] Ibid.

[44] Ciocchetti, op. cit.

[45] Ibid.

[46] Ibid.

[47] Robert M. Hunt, "You Can Patent That? Are Patents on Computer Programs and Business Methods Good for the New Economy?" Business Review, 2001, p. 7, http://tinyurl.com/h3bpyk8.

[48] In re Alappat, 33 F.3d 1526 (Fed.Cir. 1994), http://tinyurl.com/h5mxlwk.

[49] "Big Data: Seizing Opportunities, Preserving Values," the White House, February 2015, http://tinyurl.com/gqzaa5w.

[50] "S. 668—Data Broker Accountability and Transparency Act of 2015," March 4, 2015, http://tinyurl.com/jouorxp.

[51] Susan Taplinger, "DMA Expresses Disappointment with New 'Data Broker' Bill," Direct Marketing Association, Feb. 13, 2014, http://tinyurl.com/nlote3q.

[52] "S. 668: Data Broker Accountability and Transparency Act of 2015," GovTrack, undated, accessed Jan. 21, 2016, http://tinyurl.com/zzd9tzc.

[53] "Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015," the White House, undated, accessed Jan. 21, 2015, http://tinyurl.com/oydmctk.

[54] "Analysis of the Consumer Privacy Bill of Rights Act," Center for Democracy & Technology, March 2, 2015, http://tinyurl.com/h6be4wy.

[55] "CEA: Government Must Not Stifle Innovation While Protecting Privacy," news release, Consumer Technology Association, Feb. 27, 2015, http://tinyurl.com/zs7gxtj.

[56] "Statement on the Commerce Department's Consumer Privacy Legislative Discussion Draft," News release, The Internet Association, Feb. 27, 2015, http://tinyurl.com/jgntyaj.

[57] Richards and King, op. cit., p. 395.