



How Is the Internet Eroding Privacy Rights?

Stephen Currie

INCONTROVERSY



© 2014 ReferencePoint Press, Inc.
Printed in the United States

For more information, contact:

ReferencePoint Press, Inc.
PO Box 27779
San Diego, CA 92198
www.ReferencePointPress.com

ALL RIGHTS RESERVED.

No part of this work covered by the copyright hereon may be reproduced or used in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, web distribution, or information storage retrieval systems—without the written permission of the publisher.

LIBRARY OF CONGRESS CATALOGING-IN-PUBLICATION DATA

Currie, Stephen, 1960–

How is the internet eroding privacy rights? / by Stephen Currie.

pages cm.-- (In controversy series)

Includes bibliographical references and index.

Audience: Grades 9 to 12.

ISBN-13: 978-1-60152-623-6 (e-book)

1. Internet--Security measures. 2. Privacy, Right of. 3. Computer security. 4. Social media. I. Title.

QA76.9.A25C865 2014

004.67'8--dc23

2013033657

Contents

Foreword	4
Introduction	
Privacy and the Right to Know	6
Chapter One	
What Are the Origins of the Internet Privacy Controversy?	11
Chapter Two	
What Is the Effect of Social Media on Privacy?	25
Chapter Three	
How Is Data Collection Undermining Privacy on the Internet?	38
Chapter Four	
How Are Hackers Using the Internet to Violate Privacy?	52
Chapter Five	
What Can Be Done to Limit Privacy Violation on the Internet?	66
Source Notes	80
Related Organizations and Websites	84
Additional Reading	87
Index	89
Picture Credits	95
About the Author	96

Foreword

In 2008, as the US economy and economies worldwide were falling into the worst recession since the Great Depression, most Americans had difficulty comprehending the complexity, magnitude, and scope of what was happening. As is often the case with a complex, controversial issue such as this historic global economic recession, looking at the problem as a whole can be overwhelming and often does not lead to understanding. One way to better comprehend such a large issue or event is to break it into smaller parts. The intricacies of global economic recession may be difficult to understand, but one can gain insight by instead beginning with an individual contributing factor, such as the real estate market. When examined through a narrower lens, complex issues become clearer and easier to evaluate.

This is the idea behind ReferencePoint Press's *In Controversy* series. The series examines the complex, controversial issues of the day by breaking them into smaller pieces. Rather than looking at the stem cell research debate as a whole, a title would examine an important aspect of the debate such as *Is Stem Cell Research Necessary?* or *Is Embryonic Stem Cell Research Ethical?* By studying the central issues of the debate individually, researchers gain a more solid and focused understanding of the topic as a whole.

Each book in the series provides a clear, insightful discussion of the issues, integrating facts and a variety of contrasting opinions for a solid, balanced perspective. Personal accounts and direct quotes from academic and professional experts, advocacy groups, politicians, and others enhance the narrative. Sidebars add depth to the discussion by expanding on important ideas and events. For quick reference, a list of key facts concludes every chapter. Source notes, an annotated organizations list, bibliography, and index provide student researchers with additional tools for papers and class discussion.

The *In Controversy* series also challenges students to think critically about issues, to improve their problem-solving skills, and to sharpen their ability to form educated opinions. As President Barack Obama stated in a March 2009 speech, success in the twenty-first century will not be measurable merely by students' ability to "fill in a bubble on a test but whether they possess 21st century skills like problem-solving and critical thinking and entrepreneurship and creativity." Those who possess these skills will have a strong foundation for whatever lies ahead.

No one can know for certain what sort of world awaits today's students. What we can assume, however, is that those who are inquisitive about a wide range of issues; open-minded to divergent views; aware of bias and opinion; and able to reason, reflect, and reconsider will be best prepared for the future. As the international development organization Oxfam notes, "Today's young people will grow up to be the citizens of the future: but what that future holds for them is uncertain. We can be quite confident, however, that they will be faced with decisions about a wide range of issues on which people have differing, contradictory views. If they are to develop as global citizens all young people should have the opportunity to engage with these controversial issues."

In Controversy helps today's students better prepare for tomorrow. An understanding of the complex issues that drive our world and the ability to think critically about them are essential components of contributing, competing, and succeeding in the twenty-first century.

Privacy and the Right to Know

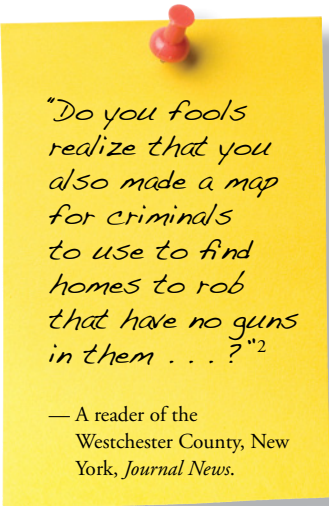
In late 2012 a suburban New York City newspaper, the *Journal News* of Westchester County, decided to run a story about gun ownership in its region—a topic sparked in part by the deadly shootings at Sandy Hook Elementary School in nearby Newtown, Connecticut, just days earlier. As part of the story, reporters contacted local governments and requested the names and addresses of people who were licensed to own handguns. The resulting story, “The Gun Next Door: What You Don’t Know About the Weapons in Your Neighborhood,” appeared in the newspaper’s print edition and was also featured in the online edition. The online edition, however, included something else as well: an interactive map of two New York counties that used circles to indicate the home of each permit holder. By clicking on the circle, users could find the name and full address of the person represented.

Getting and posting the information was perfectly legal. At the time, New York State did not offer gun permit holders any privacy assurances; under a law known as the Freedom of Information Act, in fact, county authorities were required to give the list of licensed gun owners to the newspaper. Newspaper officials were also convinced that publishing the list was of value to the community. Readers of the *Journal News*, editors asserted, “are understandably interested to know about guns in their neighborhoods.”¹ Indeed, the map received more than 1 million views, far more than any

previous article or graphic on the *Journal News* website. And in the weeks following the release of the information, the publisher stated that the newspaper had gotten a good deal of positive feedback from readers who were grateful that the newspaper had made the map available.

But many other people were appalled by the publication of the map. For many, safety was the major issue. Some thought it put gun owners in danger; according to this view, criminals seeking to steal a gun would know exactly where to go to obtain one. Others thought that the map jeopardized the safety of residents who did *not* own guns. As one reader put it, “Do you fools realize that you also made a map for criminals to use to find homes to rob that have no guns in them . . . ?”² There was particular concern about the security of women who had escaped from domestic violence, some of whom had purchased guns for self-protection; the map, the newspaper’s critics charged, made it easier for abusers to discover where their former victims were now living. And some people worried about the safety of law enforcement professionals such as police officers and prison guards, who could now be tracked down by a former prisoner seeking revenge for an arrest or perceived poor treatment in jail.

The most basic concern, however, was that by posting the map on the newspaper’s website, the *Journal News* editors had violated the privacy of hundreds of gun owners. In particular, the posting of the information online, where it could be found by anyone with a smartphone and wireless access, struck many people as misguided. The Freedom of Information Act, observers charged, was not intended to allow the wholesale posting of public records on the Internet. The law, they argued, was designed to allow a concerned citizen to go down to the county courthouse, make a request for the names and addresses of nearby gun permit holders, and perhaps share that information with a handful of equally interested people. Getting that information, in their eyes, required some effort beyond the click of a mouse. “Just because it’s available and public record,” says a professor, “doesn’t mean we have to make it so readily available.”³



“Do you fools realize that you also made a map for criminals to use to find homes to rob that have no guns in them . . . ?”²

— A reader of the
Westchester County, New
York, *Journal News*.



A police officer prepares for a training drill at a firing range. When a New York newspaper posted online the names and addresses of licensed gun owners in the area, police officers and other gun owners expressed outrage that their privacy had been violated.

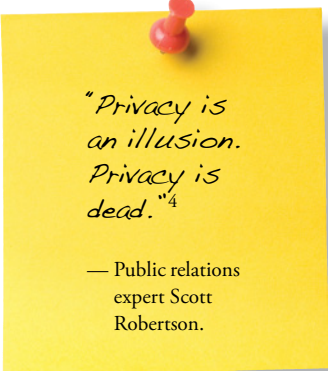
A Wider Debate

The debate raged for nearly a month. Critics of the newspaper published the home addresses of newspaper personnel and arranged a boycott of *Journal News* advertisers. Some went further: Several staffers at the newspaper were threatened, and the *Journal News* eventually hired armed guards to patrol its office space to deter potential attackers. In January 2013, however, the newspaper removed the interactivity from the map; editors said the posting had served its purpose. Around the same time, the New York state legislature—partly in response to this case—passed a bill that

would allow holders of gun permits to keep their information private. The new bill, together with the change to the map, served to tone down the specific controversy. Those who had opposed the newspaper's original decision were pleased by the outcome, if not necessarily ready to forgive the *Journal News*.

But the case of the *Journal News* is also just one part of a much larger issue: the extent to which the Internet is steadily compromising the right to privacy. As personal data of all kinds is increasingly posted or stored online by newspapers, governments, corporations, and even ordinary people, it becomes more and more difficult for private citizens to keep elements of their lives to themselves. Even when data is protected by a password or encrypted in some form, it is still online, available to be seen by a determined criminal or exposed to the world through an accidental breach of security. Viewed in this light, the *Journal News*'s interactive map is simply an example of the trend toward less and less consideration for privacy. Though the map has been taken down and the privacy rights of gun owners in New York have been affirmed, many observers would say that this is just one small victory in a bigger battle and that the Internet erodes the right to privacy in a myriad of other ways.

Although nearly everyone agrees that the right to privacy has been impacted by the Internet, Americans do not necessarily agree on the extent to which this is happening; neither do they agree on the effects of these changes. To some observers, the erosion of privacy has been limited. They believe that privacy can still be maintained even in a digital age, though safeguarding data may require more effort than before. Others, however, see the loss of privacy as inevitable. The right to privacy, in this view, is a relic of a bygone age and no longer applies to a modern web-based world. There is simply too much information stored online—information known to governments, businesses, and Internet friends—and that information is entirely too easy to access. “Privacy is an illusion,” claims public relations expert Scott Robertson, writing about the changes in the concept of privacy in the Internet era. “Privacy is dead.”⁴



"Privacy is
an illusion.
Privacy is
dead."⁴

— Public relations
expert Scott
Robertson.

Whether dead or merely ill, whether an illusion or simply somewhat obscured around the edges, there is no question that the issue of privacy is a vital one in a modern world.

Facts

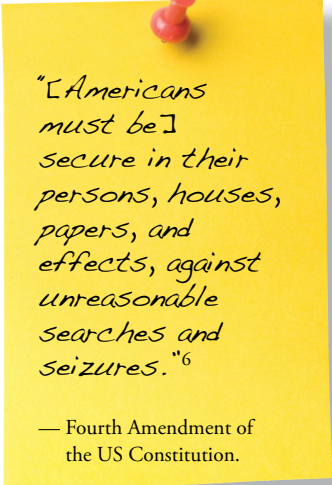
- Forty-five percent of respondents in a 2013 Fox News poll say they would not be willing to give up personal freedoms such as privacy to reduce terrorist threats, compared to forty-three percent who say they would.
- According to a 2012 study by the Pew Foundation, teenage boys are almost twice as likely as teenage girls to post their personal cell phone numbers online.
- According to a Pew Internet & American Life Project survey, fifty-four percent of mobile phone users say they have not installed certain apps on their phones because of privacy concerns.

What Are the Origins of the Internet Privacy Controversy?

The Constitution of the United States, written in the late 1700s, is the basic document that describes and defines the American system of government. The Constitution, for example, sets up a representative government with senators, representatives, a president, and a system of courts; it allows the government to levy taxes; and it describes, at least in general terms, the relationship between the federal, or national, government and the states. The Constitution also provides a framework for the laws of the United States. No law that directly conflicts with the provisions of the Constitution can remain in effect.

In addition to detailing the governmental structure of the United States, the Constitution protects Americans by listing some of the rights they are entitled to. It does this mainly, though not exclusively, with a series of amendments—additions or changes to the original text of the Constitution. In particular, the first ten amendments, known as the Bill of Rights, list some basic protections to which all Americans are entitled. These include such familiar rights as the right to free speech—that is, the right for a person to say what he or she thinks without being imprisoned for

it—and the right to a trial by a jury made up of ordinary citizens. They also include less familiar rights; the Third Amendment, for example, holds that the government may not station soldiers in the houses of Americans without the consent of the owners.



"[Americans must be] secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."⁶

— Fourth Amendment of the US Constitution.

The rights that are listed in the Constitution are not necessarily absolute. The right to free speech, for example, does not extend so far as to allow people to tell deliberate lies about others. Nor does it allow people to incite panic by exercising their right to free speech: A classic example is that people may not shout “Fire!” in a crowded theater. Similarly, the meaning of the Second Amendment’s “right to bear arms”⁵ is a matter of much dispute, and precisely what the First Amendment’s guarantee of freedom of religion means is open for debate. Defining the limits of these freedoms is a job for the US court system. In many situations the final word on what is—and is not—covered by these various amendments

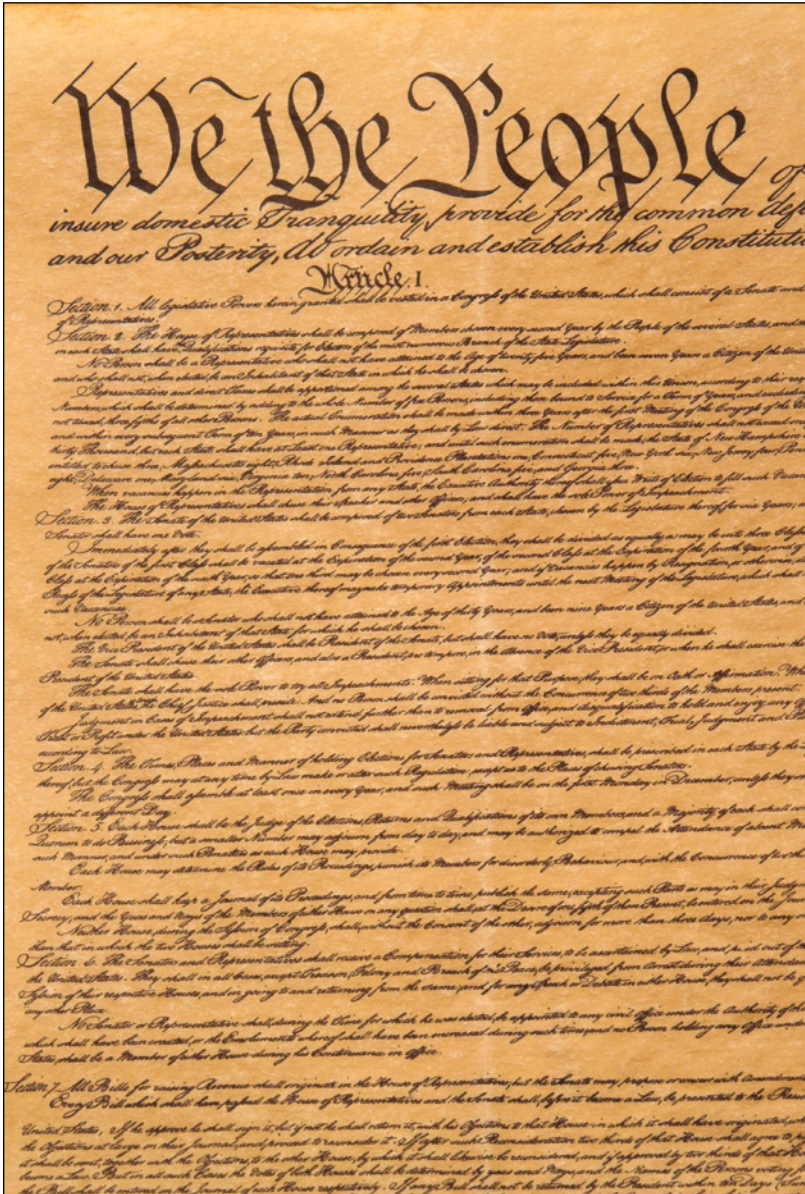
is left to the nine justices serving on the US Supreme Court, the most powerful court in the country.

The Right to Privacy

At the same time that the courts have limited certain rights, judges have also identified and protected some rights that are not specifically listed in the Constitution. Chief among these is a right to privacy. Though the Constitution does not mention this right by name, it is hinted at in several of the amendments. In particular, it forms a foundation for the Fourth Amendment. This amendment guarantees the right of the people to be “secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”⁶ In other words, the government may not send its agents to carry out random searches of Americans’ homes and possessions. While not directly naming a right to privacy, this amendment recognizes that some aspects of Americans’ lives are not the government’s business.

Equally important, courts have frequently affirmed that the right to privacy is implied by the Constitution. In 1965, for example, the Supreme Court ruled that the right to privacy was pro-

tected by a “penumbra of the Bill of Rights.”⁷ A penumbra is a shadow; the justices were saying that the rights actually enumerated in the Constitution cast a metaphoric shadow that made a right to privacy a basic part of being an American. More recent court cases have also affirmed that privacy rights are guaranteed by the Constitution. And a number of laws passed in the 1990s



The US Constitution (pictured) does not specifically include a right to privacy. Several of the constitutional Amendments imply that Americans have such a right and, over the years, it has been affirmed by the courts in various cases.

Privacy and E-mail

The issue of how private an e-mail is raises important questions. In one sense, e-mail is simply another form of a letter sent through the postal system and deserves the same protection. In this view, password-protected accounts have the same function as an envelope—that is, they make it difficult for someone other than the intended recipient to see what the e-mail says.

But in fact, e-mail is less private than many people believe. E-mails can often be intercepted and viewed by hackers—people who illegally break into databases and other websites. Companies that offer e-mail accounts often have access to the e-mails sent by their customers, and workplaces can—and often do—monitor employees' e-mails without telling the employees what they are up to. And of course the recipient of an e-mail can easily forward it to everyone in his or her address book, making the contents of the original message public whether the writer wants it to be or not.

US courts have in fact come to divergent views on the privacy of e-mails. Some courts have ruled that privacy protections apply to e-mails in general; others have ruled the opposite. Until the courts come to a consensus, e-mail users are typically cautioned to treat e-mail less as a sealed letter and more as a postcard, in which the contents are available to anyone who really wants to read them.

and beyond explicitly safeguard privacy rights in at least some circumstances. The Health Insurance Portability and Accountability Act, originally passed in 1996, is an example; it regulates access to Americans' medical records and makes it very difficult for anyone to see this information without the consent of the patient.

Like other basic rights, though, the right to privacy has limits,

and these limits are hinted at in the Fourth Amendment's wording: It bans "unreasonable searches and seizures,"⁸ not *all* searches and seizures. Most Americans would agree that there are reasonable searches and seizures and that most of these involve law enforcement. Criminal activities, after all, are generally private. Few people walk through the streets loudly announcing their plans to rob a bank or boast on Facebook about the illegal drugs they have for sale. Privacy regulations, if taken to a logical extreme, would say that law enforcement officers should never be allowed to invade privacy, even when they strongly suspect that criminal activities are being discussed, planned, or carried out. However, few Americans would be comfortable with the notion that all private activity should be completely off-limits to police officers.

As a result, law enforcement officials have traditionally been allowed to infringe on someone's personal business if they have reason to believe that person is breaking a law or contemplating breaking one. When police officers want to search a suspected criminal's home or workplace, however, they must typically obtain a warrant—an order signed by a judge allowing access for law enforcement. A similar process holds for police officers who want to listen to suspects' private phone conversations, intercept their mail, or otherwise engage in some kind of surveillance. In most cases warrants and other permissions are not given out lightly. On the contrary, police forces must present the judge with evidence that the suspect is likely engaged in criminal activity. If such evidence is not available, the judge is expected to deny the request. Though the right to privacy can be limited, then, it is still taken seriously by the government.

Privacy and Technology

Where the right to privacy begins and ends has never been completely clear, but the growth of technology has complicated those questions considerably. The Constitution, after all, was written at a time when modern technology was not only unknown but was largely unimagined. Thus, the Fourth Amendment and other privacy protections dealt specifically with physical privacy: they barred government from entering buildings, going through

people's belongings, and unsealing and reading letters written by one person to another. Other than examining the contents of a person's home, correspondence, or pockets, there was essentially no way to find out what a person was doing and therefore no other way for the government to unlawfully invade a person's privacy. The privacy protections of the Constitution, then, were sufficient for the technology of the era.

In the early part of the 1800s, however, technological progress began to change the way people thought about privacy. The invention of the telegraph was an excellent example. The telegraph, a network of wires that eventually stretched across the country, enabled Americans to send one another messages through a central operating system. Unlike letters, telegrams—the messages sent via telegraph—were very nearly instantaneous. These messages, which consisted of electrical impulses that could be translated into words, arrived at their destinations almost as soon as they were sent. During the mid-nineteenth century, sending a telegram was by far the best option for a person who wanted to contact a friend, relative, or business associate as promptly as possible.

But telegrams were not offered the same privacy protections as letters. People did not have their own telegraphs at home; instead, they had to go to a telegraph station and write out the message for the operator. The operator would then translate the message into electrical impulses and send it through the wires. The reverse happened at the other end, where another operator received the message, translated it back into words, and wrote it out for the recipient. Whereas a letter could be sealed so it would not be seen by anyone other than the writer and the person to whom it was addressed, the same was not true of a telegram. Besides the sender and the receiver, then, at least two telegraph operators knew the contents of every telegram sent in the United States.

As a result, telegrams were not actually private at all. A person who sent sensitive information through the mail could expect that the Constitution would protect his or her privacy. Unless they got a warrant, law enforcement officials had no legal way of knowing what was in the letter. The telegram, however, was different. If Americans sent telegrams that boasted of committing crimes,

they risked arrest. Some telegraph operators willingly alerted the authorities when they encountered telegrams that they considered questionable. And when operators did not reveal the contents of these messages, government officials frequently forced them to do so. While in one sense telegrams were simply another form of a letter, then, they were treated differently from ordinary mail by both telegraph operators and the law.

More New Technologies

Telegrams were perhaps the first example of how technological change complicated privacy laws. They were not, however, the last. The telephone began arriving in American homes and businesses toward the end of the 1800s, and law enforcement officials soon

Telegraph messages traveled much faster than letters, but they were not private. They passed through the hands of an operator on each end and sometimes other staff before reaching the intended recipient.



realized that they could track what numbers people called or even secretly listen in on citizens' conversations, a process known as wiretapping. Like telegrams, telephones were not originally covered by the Constitution's privacy protections. Since wiretapping did not necessarily involve entering someone's home or removing anything from a person's private space, it was not covered under the Fourth Amendment's ban on unreasonable searches and seizures. As a result, many people were arrested and convicted of crimes based on evidence collected via wiretapping.

Indeed, telephone conversations were not fully protected by privacy laws until a Supreme Court decision handed down in 1967—nearly a century after the first working telephone was developed. In that case, known as *Katz v. United States*, a man named Charles Katz used a pay phone for the purpose of gambling, which was in violation of the law. The FBI knew what was going on because of a device it had installed on the outside of the phone booth. Katz was arrested but argued that his right to privacy had been violated. Though the FBI asserted that it had every right to use technology to listen to Katz's conversation without a warrant—it had not entered his home, nor had it taken anything that belonged to him—Katz countered by claiming that the Constitution was designed to cover situations like his. The Supreme Court agreed, ruling that in situations where people had a “constitutionally protected reasonable expectation of privacy”⁹—such as in a phone booth with the door closed—the Fourth Amendment should apply.

The *Katz* case settled the question of whether privacy laws covered telephone conversations, but it went further as well. By ruling that the Fourth Amendment could be applied to cases in which there was no physical invasion of privacy, the court also suggested that new technologies as yet unknown in 1967 might be governed by existing privacy rights as well. And some court decisions since the *Katz* case have followed this principle. In 2001, for example, Oregon police used a thermal imaging device, which measures the amount of heat radiating from a building, to determine that a man was illegally growing marijuana plants on his property. The man's initial conviction was overturned, however, when the Supreme Court ruled that use of the imaging device constituted a

What the Constitution Does Not Protect

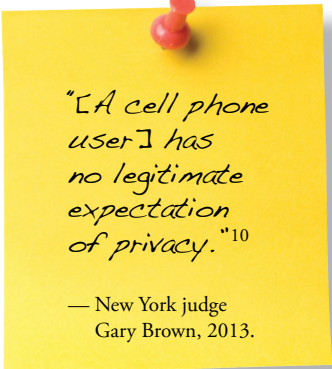
The rights enumerated in the Constitution deal only with what the government may and may not do. The statement in the First Amendment that the right to free speech must not be infringed, for example, forbids Congress from passing a law designed to do this. But the Constitution is silent about the question of what other people may do. The right to free speech does not make it illegal for a radio station, say, to fire a host who uses offensive language, or for a sports team to discipline a player who openly criticizes management.

That is true of privacy rights as well. Though the Constitution protects the right to privacy to at least some degree, it only outlines what government may or may not do. Because of this, for example, businesses can and do try to collect information on their customers without running afoul of the Constitution. The right to privacy implied in the Constitution is therefore of no help in combating the collection of data by businesses or the monitoring of employees' communications by companies. While governments at various levels may decide to limit the ability of corporations to collect such information, they are not required to do so by the Constitution.

search under the terms of the Fourth Amendment; thus, police officers needed to obtain a warrant before using the device, which they had not done.

In other cases, though, courts have ruled that privacy rights do not apply, given certain uses of new technologies. Courts have generally ruled, for instance, that appearing in a public place means sacrificing privacy protections. A person in an arena, on a sidewalk, or in a store, for example, cannot reasonably expect privacy. Thus, a person who commits a crime on a public street and is

caught by a security camera probably cannot have the case thrown out of court on the grounds that the presence of the camera represented an invasion of privacy. Similarly, a person who is shown in the stands at a baseball game during a national TV broadcast cannot claim that the TV network invaded his or her privacy by showing that person's picture on the air—which the fan might be tempted to do if, say, he or she had skipped work to go to the game and was subsequently fired after being spotted on the broadcast.



"[A cell phone user] has no legitimate expectation of privacy."¹⁰

— New York judge
Gary Brown, 2013.

Even in the case of telephones, privacy is not necessarily a given. Although the *Katz* case protected the content of conversations, the Supreme Court later ruled that law enforcement officers did not need a warrant to obtain a list of the numbers called by a particular phone. In the estimation of the justices, callers should not expect to be able to keep the fact of these calls private, even if the content of the calls was protected. Conversations held over speakerphones, similarly, may not qualify

for full privacy protections. And cell phones occupy a category of their own. In a May 2013 decision, for example, New York judge Gary Brown ruled that law enforcement agents could track a person's whereabouts by monitoring the position of his or her cell phone. As long as the phone was switched on, Brown ruled, using this information was entirely legal. Unless the cell phone user has actually powered the device off, the judge explained, a phone owner "has no legitimate expectation of privacy."¹⁰

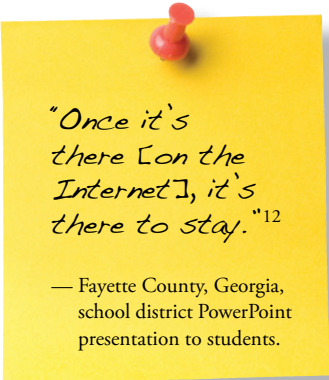
The Internet

The new technology that has had the greatest impact on privacy rights, however, is unquestionably the Internet. In the world of the twenty-first century, an enormous amount of data about individual people is stored electronically, much of it in easily accessible lists called databases. Most municipalities keep elections data online, for example, including voters' names, addresses, birth dates, and sometimes their political party preference. Businesses keep tabs on their customers and what they buy; companies like the online retailer Amazon frequently send out personalized e-mails recommending

products based on an individual customer's purchasing history. And social media sites like Facebook can provide a record of what a person has been doing and thinking over a period of months or years, all of it available with just a few clicks of a mouse button.

These records are extremely useful. Electronic data is so easy to access that it can save governments and businesses enormous amounts of money, time, and energy, not to mention shelf space. Digitizing records such as voter registration rolls can replace literally dozens of physical books filled with registration cards, and Facebook records are much simpler to go through than a box of letters would be. Few Americans would want to go back to a pre-Internet way of life in which information was harder to find, store, and sort—a world without a search function. As one writer only half-jokingly puts it, imagining a world without the Internet is “akin to thinking about your dog being eaten alive by an alligator before your very eyes.”¹¹ The Internet is not only fun, it offers efficiency and convenience as well.

But the power of the Internet is double-edged. The detailed information available online often includes personal data that many people might prefer not to have accessed. In some cases the information may not be secure and may fall into the hands of someone other than the people who gathered it. In some cases the information has been obtained without the consent of the person it pertains to. And sometimes the information is of the kind that people might want to have remain online for a time, but not necessarily forever. This is particularly common with social media such as Facebook and Twitter, where a post that seems clever and witty at one point in a person's life may seem stupid or humiliating a month or a year afterward. Unfortunately, social media posts rarely, if ever, disappear completely. As one school district in Fayette County, Georgia, cautions its students, “Once it's there [on the Internet], it's there to stay.”¹²



*“Once it's
there [on the
Internet], it's
there to stay.”¹²*

— Fayette County, Georgia,
school district PowerPoint
presentation to students.

Privacy Problems

The Internet thus presents two major issues where privacy is concerned. One is the increasing amount of personal data stored



A doctor reviews a patient's medical history. Huge amounts of personal information are stored online by banks, retailers, schools, hospitals, and various government agencies.

online. As electronic databases grow, the number of pieces of information regarding any one individual increases dramatically. Much of this information is collected and kept by the private sector. Retailers keep records of purchases, hospitals store information about medical histories, and banks can access details of a customer's financial situation quickly and easily. Government, too, stores information online: the Internal Revenue Service keeps track of personal income, public schools have databases of grades and test scores, and the Social Security Administration lists every American's date of birth and Social Security number. Some of this information could be misused by the corporations or government agencies that keep it, a prospect that worries many citizens. Moreover, this information might be available to hackers, people who break into poorly secured databases and steal what they can. The prospect of hacking also is of great concern for many Americans.

The other issue is that breaches of privacy can now be broad-

cast quickly and simply around the globe. Since the early 1990s, thanks to the Internet, the number of people who can view any given piece of information has increased exponentially. Today, a photo of a drunken teenager in an embarrassing pose can at least in theory be viewed by millions of people, and photos and Facebook posts of this sort have caused people to lose jobs, spouses, and friends. In addition to the number of people who see data, the speed at which data travels via the Internet is a concern. A stolen credit card can be used a dozen times or more online before the owner knows it has disappeared. The rise of the Internet has led to many cases in which privacy has been compromised in ways that would have been impossible—or at the least very difficult—in the years before the Internet’s existence.

Much has changed since the United States took steps to safeguard a basic right to privacy by approving the Fourth Amendment. A steady stream of new technologies beginning in the early 1800s changed the way people live, work, and play, and this stream of new inventions became a torrent in the early twenty-first century. The American legal system, not designed for rapid social and technological changes, has had a difficult time keeping up. Today technological innovations are covered by a patchwork of laws—and are at the heart of the debate over the right to privacy and the extent to which it is being infringed in modern society. Nowhere today does that debate rage more brightly than in the realm of the Internet. But as the historical record makes clear, the roots of the conflict lie many decades in the past.

Facts

- The phrase “penumbra of the Bill of Rights” was originally used by the US Supreme Court in deciding the 1965 case *Griswold v. Connecticut*, establishing a woman’s right to obtain contraceptives.
- The first federal law to address wiretapping of telephone conversations was passed in 1934.
- According to a 2013 survey by On Device Research, about 10 percent of people on social media have lost jobs because of something they posted on their accounts.
- A 2005 University of Pennsylvania study found that 20 percent of respondents did not know that companies are able to track their online customers’ activities on the Internet.
- The Social Security Administration began computerizing its records in the 1950s; by 1962 the bulk of records were stored electronically.

What Is the Effect of Social Media on Privacy?

One of the great innovations of the 1990s and beyond is the sudden and rapid growth of social media, or social networking sites, which permit people to communicate quickly and easily through the Internet. The best-known example of social media in today's world is Facebook. Founded in 2004 by several college students, most notably Mark Zuckerberg, Facebook allows users to keep in close contact with one another by creating a personal profile, uploading photographs, posting messages, and adding other users as friends, among many other activities. As of the summer of 2013, Facebook boasted more than 1 billion active users—about one-seventh of the world's population. While that figure includes many people who rarely visit the site, it also encompasses millions who use Facebook daily or almost daily, often checking it regularly throughout their waking hours.

Facebook may be the most famous online networking site, but it is by no means the only one. Facebook was preceded, for example, by similar sites such as Myspace, which also provided users with pages of their own and allowed them to interact with other users through posts, photos, and more. In many ways Myspace

“I Give God 10%”

In January 2013 a customer at a Missouri restaurant decided not to leave a gratuity for the waitress who served her party. She crossed out the suggested 18 percent tip on the credit card slip, wrote “0” in the space provided for an additional tip, and recalculated the bill without the gratuity. Then she wrote a note on the slip: “I give God 10%[.] Why do you get 18[?]”

The waitstaff at the restaurant found the comment offensive. Another server photographed the credit card slip and posted the photo to the social media site Reddit. Within a matter of days thousands of people had seen the post, and it was appearing on Facebook and other social media sites as well.

The author of the note was soon identified as the pastor of a local church. At first the pastor responded to the posting of her writing by complaining to the restaurant about the violation of her privacy. Later, though, she seemed to recognize that the note was inappropriate. “My heart is really broken,” she told an interviewer. “I’ve brought embarrassment to my church and ministry.”

The case sparked a debate about privacy. Some observers argued that the server had no business posting the note; it was an invasion of the customer’s privacy. (The restaurant agreed and fired the server.) Others, however, argued that the pastor deserved public shaming and that the posting on Reddit was entirely acceptable. What is certain is that such a controversy could not have taken place before the rise of social media.

Quoted in Smoking Gun, “Pastor Apologizes for Snide Remark on Meal Receipt,” January 31, 2013. www.thesmokinggun.com.

has been superseded by Facebook, but it remains a popular site, especially among musicians and gamers. Another site, LinkedIn, focuses on connecting people professionally. More recently, Twitter has come onto the scene. Twitter enables users to communicate with large numbers of interested people, known as followers, by sending out short messages—known as tweets—about their activities, thoughts, and experiences. Some celebrities' Twitter accounts have hundreds of thousands of followers.

Social networking also includes a host of other types of sites as well. Blogging, for example, came into vogue in the 1990s and is still popular today. Bloggers write short paragraphs or longer essays about subjects that intrigue them and post them to a website, where they can be read by other interested people. Though blogging is less immediate than Twitter, it is much more in-depth and can be an excellent way for people to communicate their ideas. Social media also includes photo- and video-sharing sites such as YouTube and Flickr; online message boards where people discuss topics of interest to them, often posting under made-up screen names rather than using their actual identities; and general-interest sites that allow people to share information and ideas about a variety of subjects. A popular site called Pinterest, for example, bills itself as “a tool for collecting and organizing things you love.”¹³

Effect on the World

Social media has had a remarkable effect on society. Sites such as Facebook and Twitter permit users to share their thoughts with dozens or even hundreds of friends and followers, including people they know very well in real life—and, frequently, including some they know only through their online activities. Athletes send out tweets giving the results of their games, pet owners upload videos of their dogs and cats to YouTube, cancer patients seek one another out on message boards dedicated to coping with the disease. Businesses use Facebook to advertise their products, and political pundits are as likely to post their predictions and analyses in blog form as they are to publish them in traditional magazines or newspapers. These updates and postings are instantaneous, or very nearly so, and they have changed the way people think about

communication and the world around them. As blogger Kenneth Wisnefski writes, “It’s hard to imagine a time when people weren’t so well connected.”¹⁴

In many ways the rise of social media has been positive. Facebook, in particular, has been credited with helping topple dictatorships in Egypt and Tunisia in 2010 and 2011. As demonstrations against the governments became more intense, Facebook permit-

ted protesters to communicate with each other and with the general public. One Tunisian activist, a journalist reported, spent “18 hours a day in front of his computer running a Facebook page that [became] one of the primary sources of information on the protests.”¹⁵ Similarly, after the Boston Marathon bombing in April 2013, friends and family members of runners and onlookers were able to use social media to get up-to-date information about their loved ones. And in general, social media has been of great benefit to shut-ins, people with arcane interests not widely shared by others in their geographic area, and people who wish to reconnect with friends and relatives.

But the prevalence of social media has its drawbacks as well. It has been used to promote criminal activity; sexual predators, for example, have been known to use Facebook and other social networking sites to find victims. Just as social media sites have been a force for freedom in some countries, too, they have also been used by repressive governments to keep tabs on their citizens. “Facebook is a great database for the government now,”¹⁶ says exiled Syrian activist Ahen al-Hindi, who is concerned that Syria’s rulers are using social media to help find and arrest their political opponents. But perhaps the biggest debate over social networking involves questions of privacy. As many Americans see it, social media has erased boundaries between what is public and what is private—and has done so to the great detriment of social media users and the general public alike.

Oversharing

As different forms of social media have grown, one common criticism is that they lead to what some people call oversharing—that



“It’s hard to imagine a time when people weren’t so well connected.”¹⁴

— Kenneth Wisnefski,
CEO of technology
company Webimax.



is, providing readers or listeners with more information, and in particular more personal information, than they need or want. Oversharing has always been possible in ordinary living, through face-to-face conversations and telephone calls. But there is no question that the rise of social networking has increased incidents of oversharing. In many cases the information shared is benign. Blogs, Facebook posts, and tweets are full of trivial information along the lines of what color socks the writer is wearing or what the author's pets are doing at any given moment. "No one cares what you ate for breakfast"¹⁷ is a standard rule for would-be bloggers and tweeters, but the need for such a rule makes it clear how often it is ignored. Of course, it is easy enough for readers to ignore mundane postings of this sort.

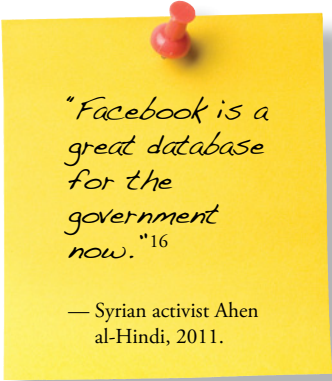
Unfortunately, not all of the oversharing common on social media today is harmless. Some of it moves into areas that are highly sensitive in terms of privacy. "More than ever," states blogger Jon Green, "[social media] users are making a wide array of infor-

Emergency personnel aid injured people at the finish line of the 2013 Boston Marathon after an explosion. Worried friends and family members used social media to share whatever information they could get about race participants and spectators who were in the area of the blast.

mation including our preexisting health conditions, plans for the day, phone number and personal finances public and available.”¹⁸ These tweets and postings can be detrimental to those who posted them—and occasionally to others as well. Though social media has been around for only a few years, thousands of Americans have found out the hard way that posting information online that is humiliating, overly personal, or simply not well-thought-out is a bad idea. The ease with which people can compromise their own privacy and the privacy of others is perhaps the biggest downside to social networking.

Much of the harm caused by social media posts comes of poor judgment. Though social media users may wish to keep their followers and friends up-to-date about various aspects of their lives, it is not wise for them to tweet or post potentially sensitive information. Unfortunately, that can include many items that seem at first glance to be quite harmless—but are not, depending on who happens to see the information. A Facebook user who provides updates on her health, for example, may find that her new employer, worried that she will miss too many work days to treat her illness, decides to fire her. A Twitter user who tweets about his vacation may come home to find that his house has been burglarized while he was away. And Myspace or LinkedIn members who post their birth dates online may discover that somebody has used that information to steal their identities.

Many social media sites provide privacy settings, which enable users to limit access to this type of information only to people who have been designated as “friends.” Over a quarter of all Facebook members, however, make essentially no use of privacy settings. Thus, anyone who is curious can access this information. In Green’s words, failing to use strict privacy settings on social media sites is akin to freely sharing information with “employers, insurers, the IRS, divorce lawyers and criminals.”¹⁹ Moreover, even people who use privacy settings cannot be certain that their information does not reach a wider audience. People who are on Twitter, for example, often retweet each other’s messages—that is, they send them along to other friends and followers, allowing the



“Facebook is a great database for the government now.”¹⁶

— Syrian activist Ahen al-Hindi, 2011.

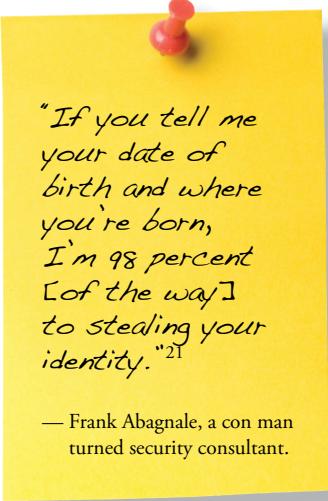
tweet to reach people who are not on the original sender's list of friends. In this way even privacy settings cannot guarantee that information will remain truly private.

Credit Cards, Photos, and Security

Indeed, there have been many examples of people who shared too much online—and regretted it. Some people have been known to post photos of their credit cards on social networking sites, with names and numbers clearly visible. “Got my new debit card today!”²⁰ a member of a social networking site posted in June 2013, with the message accompanied by a full photo of the card. But loss of privacy can be the result of much less obviously compromising information than a credit card. Often, for instance, birthplaces have been used by thieves to capture a person's identity. “If you tell me your date of birth and where you're born [on Facebook],” says Frank Abagnale, a former con man who now works as a security consultant, “I'm 98 percent [of the way] to stealing your identity.”²¹

Sometimes the information posted does not seem specifically personal, but it can compromise privacy nonetheless. One example involves common security questions designed to make certain that someone wanting access to a website is who he or she claims to be. The names of pets or elementary schools, for example, are frequently used to check identity, the theory being that only the account holder knows the answer. That may once have been true, but Facebook and similar sites have changed things. “If you're like me,” reports a blogger, “you probably share pictures of your pets . . . with cutesy captions like, ‘Look at Bella sitting in the flower pot!’ While you may see these posts as a quirky way to share your life with friends across the country, criminals take note of your cat's name—and see if they can use it to crack your password.”²²

People who use social media can unknowingly jeopardize their privacy in other ways as well, especially as the pace of technological progress increases. Some experts today even caution social media users against putting photos of themselves online. In one recent



*“If you tell me
your date of
birth and where
you're born,
I'm 98 percent
[of the way]
to stealing your
identity.”²¹*

— Frank Abagnale, a con man
turned security consultant.



People who foolishly post photos of their credit or debit cards on social networking sites, as some have, are asking to be victims of identity theft. The posting of too much personal information online is an ongoing problem.

study, researchers were given photos of randomly chosen college students. Using facial-recognition software, they matched the faces to pictures posted on sites like Facebook and were eventually able to attach names, dates of birth, and occasionally even Social Security numbers to the faces by using online data. Of course, posting a photo is much less risky to privacy than posting a birth date or a Social Security number, and carrying out all these steps is sufficiently complex that not just any hacker or identity thief can do it. Still, as one of the study's authors points out, "The ingredients of the recipe we used are not secret. Everyone has access to them."²³

Work, Marriage, and the Law

Another significant privacy issue with social networking involves the indiscriminate posting of messages and pictures. Facebook and other social media sites have been used in court many times. In one recent case, for instance, a woman claimed in court that she had never smoked marijuana—but her Facebook page had pictures of her engaging in that very activity. In a similar case, this one involving divorce, a woman accused her husband of infidelity, a charge

that he denied. “The guy testified that he didn’t have a relationship with this woman,” the woman’s lawyer explains. “They were just friends.” A quick visit to the supposed girlfriend’s Facebook page, however, revealed pictures of her with the man in poses indicating that they were certainly more than just friends. “The girlfriend hadn’t put security on her page,” the lawyer continues, “and there they were.”²⁴ Situations like these are so common that some divorce lawyers forbid their clients from posting on social media sites at all.

What a person does on social media can damage his or her job prospects as well. Sometimes the issue is offensive postings. In one well-publicized case, Chicago airport screener Roy Egan was fired for posting anti-Muslim, antigay, and anti-African American messages on his Facebook page. Though no one accused Egan of posting during work hours, his page identified him as an employee of the Transportation Security Administration. Not wanting to be associated with Egan’s opinions, the agency eventually determined that Egan’s posts violated its code of conduct, which applied both on and off the job. In a pre-Internet world, it is possible that Egan’s opinions would have escaped notice; but in a world of social networking, they came to the attention of his superiors—and resulted in the loss of his job.

Other cases of people being fired for social media activity involve posts that may have been made in jest but that did not come across that way. In one example, several airline employees in England were terminated after making jokes on Facebook about airline safety—including joking that the company’s airplanes had defective engines that needed frequent replacement. Still other examples have to do with criticizing or embarrassing an employer in a social networking post. In the spring of 2013, Georgia school bus driver Johnny Cook was fired after condemning his school district’s lunchroom policies in a Facebook post. And Andrew Kurtz, hired by the Pittsburgh Pirates baseball team to wear a mascot costume, was fired after writing a social media post critical of a decision made by ownership. As in Egan’s case, these jokes, opinions, and criticisms might have been kept private even a decade ago; today, however, the increasing use of social media, however, allowed them to spread across the Internet.

Backlash?

As a general rule, young adults and teenagers are more likely than older Americans to engage in oversharing online. In early 2013, however, a study carried out by television channel MTV cast some doubt on this piece of conventional wisdom. After surveying many fourteen- to seventeen-year-olds and looking closely at the data collected, MTV concluded that people in that age group are much more concerned with privacy than anyone had previously suspected. In particular, fourteen- to seventeen-year-olds were less interested in Facebook than their elders. Instead, they tended to seek out more private sites such as Instagram and Snapchat, which allow users to take a picture or a video and send it to one or more friends. Unlike Facebook, these sites are designed to make the pictures or videos unavailable to anyone but a few selected friends; in a sense, there is an automatic privacy setting. In Snapchat, moreover, the picture disappears shortly after it is opened by the recipient, leaving less of a trace than a Facebook message or a picture posted to some other website.

Not all researchers accept MTV's findings, however. Some other studies have found no such drop in the number of Facebook users in this age range. Others attribute any drop to factors that have little or nothing to do with privacy concerns—most notably a feeling among many teens that Facebook is too heavily populated with adults.

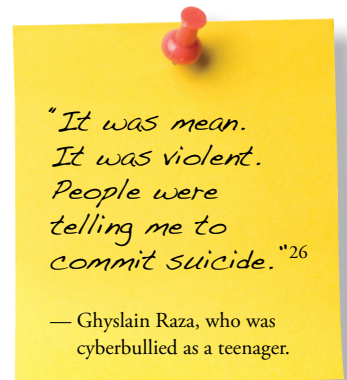
Some people who have lost jobs after rude, offensive, or critical postings were not using privacy settings when they posted. At least in theory, they were willing to allow anyone to look at what they wrote; in this view, it was their own fault that their employers read their posts. Others, however, *did* use privacy settings designed

to keep employers and others from seeing the posts in question. These people had an expectation that their posts, intended only for members of a certain group, would remain private within that circle. In most of these cases, someone who had friended the poster sent the message on to the boss, thereby infringing—morally, though not legally—on the author’s expectation of privacy. “We forget that we are not in the company of friends when we say or write the things we do” online, writes college lecturer Billie Hara. “Almost anyone can read our words, and they might misunderstand our intent.”²⁵

Harassment

Indeed, some of the most egregious violations of online privacy have to do with people violating each other’s privacy. This often takes the form of passing a post or picture on from one group of people to another. This can be innocent, but it can also be done maliciously. One classic example, dating from the early years of social networking, involves Ghyslain Raza, a Quebec youth then known mainly as the “Star Wars Kid.” For his own enjoyment, Raza videotaped himself pretending to swing a light saber. Fellow students found the tape, however, and posted it on the Internet for the purpose of mocking Raza. Over the next few months, the tape was viewed millions of times—causing Raza great embarrassment. Other classmates recognized him, and he was suddenly a public figure; his privacy was gone. “It was mean. It was violent,” Raza, now in his mid-twenties, recalls today. “People were telling me to commit suicide.”²⁶

Today this type of activity—posting pictures, videos, or messages regarding other people without their consent—is a specific type of harassment often known as cyberbullying. Cyberbullying is similar to traditional bullying, but its reach is considerably larger. Thus, the damage that can be caused is greater. In some cases cyberbullying simply consists of posting an existing embarrassing picture or video, as happened with Raza. In other cases bullies snap pictures of their victim in a compromising pose and post the pictures without the victim’s knowledge or permis-



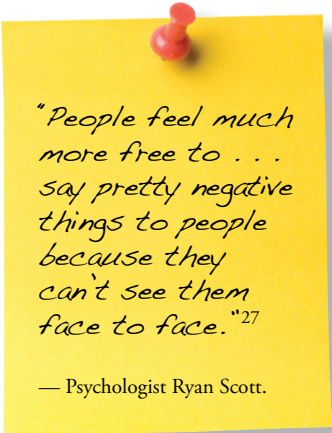
sion; this is especially common when the victim is drunk. And in still other cases, cyberbullying includes deliberately posting insults and lies about people. In one well-known case, fifteen-year-old Phoebe Prince of Massachusetts killed herself after being repeatedly called a slut—and worse—by a group of bullies on Facebook.

Cyberbullying is most common among teenagers, but adults have also been known to use the Internet to hurt others. In one case a man angry that his girlfriend had left him posted pictures of her in revealing poses on Facebook. In another a woman competing with a coworker for a promotion used social media to falsely accuse her rival of unethical conduct. Such behavior is especially common in contexts where people can remain relatively anonymous. Indeed, people have been known to create a Facebook page

with a fake identity, so it is sometimes unclear just who is carrying out the harassment. “People feel much more free to . . . say pretty negative things to people because they can’t see them face to face,”²⁷ says psychologist Ryan Scott. Regardless of whether the identity of the harasser is clear or not, though, making unwanted pictures or information available to anyone with an Internet connection is clearly a violation of the victim’s privacy.

Bullying and harassment have always been a part of life, and there is nothing new about the impulse to shame or embarrass an enemy. Long before the Internet was invented, children and teenagers found hundreds of ways to exclude and humiliate classmates and neighbors, and whispering campaigns against coworkers and managers have been a part of workplace culture for years. In this sense, cyberbullying and other forms of online persecution do not represent much of a change. But in the past the number of people who knew about the humiliation or lies would have been quite small; in most cases it would not advance much beyond a single workplace or a small circle of friends. Today, in contrast, the power of the Internet makes it possible for friends, acquaintances, future employers, and strangers to know all kinds of things about a person that the person would have preferred remain private.

The same, of course, is true of people who post too much



“People feel much more free to . . . say pretty negative things to people because they can’t see them face to face.”²⁷

— Psychologist Ryan Scott.

about themselves online. Again, there is nothing new about over-sharing. Even without the Internet, people are often quite careless with their credit card numbers, talk openly about potentially embarrassing situations, and may even boast about their petty crimes. The difference is that without the Internet, these slips go no further than the people in the room at the time and in most cases leave no lasting consequences, whereas in an Internet world these lapses in judgment may remain on display forever—and may be accessed by anyone online. In this way the Internet is not just a means of eroding privacy; it is actually a cause of privacy violations.

Facts

- According to Nielsen, between 2005 and 2007 Myspace was the most-visited social networking site on earth.
- Facebook users between the ages of eighteen and twenty-four have an average of slightly more than five hundred “friends”—the largest number for any age group, according to ArbitronEdisonResearch.
- Ninety-four percent of all teenage social media users in the United States have a Facebook account; just 26 percent are on Twitter.
- More than half of American teenagers post their e-mail address on social media sites, more than 70 percent post the name of their town and school, and one teenager in five posts his or her cell phone number.
- Just over 50 percent of students report having been victimized by cyberbullying. Half of these report that they are repeatedly bullied online or via cell phone.

How Is Data Collection Undermining Privacy on the Internet?

The Internet is both fun and informative. Gamers go online to play *World of Warcraft* and other role-playing games in which they compete with opponents from all across the world. Sports fans watch games on the Internet and visit sports sites to check their favorite teams' schedules and statistics. News junkies log on to sites such as CNN and seek out political commentary in online magazines. Tweets from celebrities are extremely popular, and there is no shortage of sites devoted to discussions of television shows, movies, and other aspects of popular culture. *Wikipedia*, a user-written online encyclopedia, offers more than 4 million articles on subjects ranging from weather patterns to rap music; as one writer puts it, *Wikipedia* promises "hours of fascinated clicking."²⁸ And of course Facebook and other social media sites attract enormous numbers of users.

With the entertainment value of the Internet as high as it is, it can be easy to forget that the Internet is also used for more mundane purposes. In particular, the Internet is often used to-

day for business-related activities such as shopping, paying bills, and dealing with the government. Well over half of all Americans, for example, make at least occasional purchases online, and many spend thousands of dollars each year over the Internet. In 2012 about 8 percent of all retail sales were made online. That includes some well-known retailers, such as Amazon, that do all or almost all their business on the Internet; but it also includes retailers that maintain physical stores, such as Sears, Walmart, and JCPenney, which increasingly sell goods online as well. In addition, growing numbers of Americans file their income taxes online, and nearly all banks offer bill-paying capabilities through their websites. From buying stocks and selling collectibles to paying taxes and renewing car registrations, the Internet is at least as valuable for business purposes as it is for having fun or learning new information.

The use of the Internet for business and government transactions presents several issues, however. In particular, it brings up

Online shopping offers consumers convenience as well as access to items that might not be found locally. At the same time, online retailers, such as Amazon, collect detailed information about the interests and buying habits of their customers.



questions surrounding personal data—and personal privacy. In order to process business transactions, companies and governments need to collect and store a great deal of private information about people, from credit card numbers and home addresses to buying habits and family size. Whereas information of this kind was once kept by hand, it is now increasingly kept online, typically in the form of databases—massive lists that can be accessed and sorted in dozens of different ways. The fact that retailers and governments collect so much information about Americans is of great concern to some privacy advocates. And even those who are not necessarily worried about the amount of information in these databases are nevertheless unhappy with how the data is collected—and how it is used. Indeed, what companies and governments know, and should know, about the private lives of Americans is a major issue in the debate over online privacy.

Corporations

Corporations collect an enormous amount of data on their customers, mainly though not exclusively through online transactions. Whereas people can make anonymous cash purchases at a brick-and-mortar store (the term *brick-and-mortar* is sometimes used to refer to a physical store in contrast to a website belonging to a retailer), anonymity is much more difficult when buying goods online. In order to make almost any kind of purchase on the Internet, it is necessary to provide a retailer with a name, a home address, an e-mail address, and a credit card number—complete with expiration date and security code, a three-digit number found on the back of the card. Sometimes telephone numbers are required as well. The information collected may be destroyed after a few days, depending on the retailer—but more often it is not.

This information is especially likely to be stored if a customer orders from a given website more than once. Rather than typing in each piece of data from scratch each time, customers generally find it more convenient to access their information by logging on to the site with a user name and password. That convenience, however, requires that the information be stored in an online database. Typing in the correct user name and password will instantly bring

Google Street View

In recent years the technology company Google has sent vehicles along virtually every American street and roadway—and many roads in Canada, Europe, Mexico, and elsewhere as well. The vehicles are there to film the houses and other buildings on each side of the road. This information has been combined with detailed maps to produce a product called Google Street View.

Google Street View is undeniably fascinating. Web users can type an address into the program and see the property on their computer screens. The program is interactive; users can navigate along the road in any direction to see neighboring houses and nearby businesses. Viewers also enjoy seeing what the cameras captured while filming. A picture of a property in Toronto, Canada, for example, shows a burning van in a driveway.

At the same time, the existence of Google Street View has led to serious questions about privacy from people who would rather not have their homes be pictured online—especially with the address attached. Since the faces of individual people sometimes appear in the pictures, too, privacy may be doubly violated. To date, Europeans have been more vocal in safeguarding their privacy rights from Google Street View than Americans. In one German city, for instance, many residents have affixed stickers to their doors declaring their properties off-limits to filming, and one Frenchman sued Google after a camera caught him urinating in his front yard. Whether the anti-Google sentiments in Europe will translate to America remains to be seen.

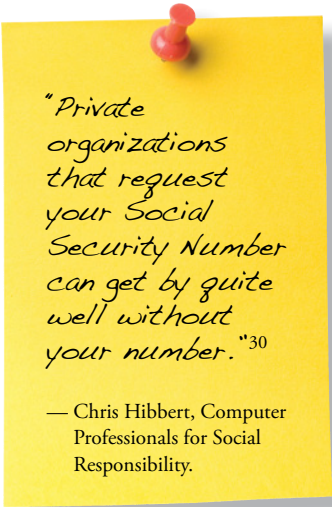
up all the data associated with the customer. Over time, moreover, this information can grow. If a customer has merchandise shipped not only to his or her house but also to other locations—as pres-

ents, say—the database will probably store these other addresses as well. And customers who make many purchases often put in a second credit card number in addition to the primary one.

Other information can wind up in the database, too. Passwords are easily forgotten, for example, so most retailers make it possible to request that the password be sent to the e-mail address on file. However, there is no guarantee that the person making the request is the actual account holder. It is possible, though not likely, that a third party has fraudulently obtained the customer's user name and has accessed the customer's e-mail account. In that case sending the password would be a very bad idea. Accordingly, websites ask account holders to answer one or more chal-

lenge questions when they set up their accounts. These are personal questions such as "What elementary school did you attend?" or "What was the last name of your best friend in high school?"—questions to which only the account holder should know the answer. When a password has been forgotten, the software prompts the requester to answer one of these questions. Knowing the answers to questions such as these, of course, gives the business even more information about the customer.

Finally, many businesses keep track of the purchases individual customers have made online. This allows companies to engage in targeted advertising—that is, letting people know about new products that might be of particular interest to them. A customer with a history of buying lots of woodworking equipment from an online department store, for instance, might be alerted via e-mail when there is a special sale on saws, chisels, and vises. An online bookseller might inform a customer who has purchased several historical mysteries within the past year that a book about crimes in Elizabethan England is now available. Many online shoppers have received e-mails such as this one from Sears that begin, "As someone who has purchased a [type of product] you may be interested in . . . ,"²⁹ followed by a list of related products, such as dishwashing soap for a customer who bought a dishwasher or pet grooming supplies for someone who has ordered pet food.



"Private organizations that request your Social Security Number can get by quite well without your number."³⁰

— Chris Hibbert, Computer Professionals for Social Responsibility.

Perhaps more seriously, customers who set up online accounts for businesses are often asked for information that might seem to have little to do with the purchases they make. Chief among these are the Social Security numbers that are issued to every American by the federal government. Social Security numbers are often used for identification purposes, but they are specifically designed to determine eligibility for certain government benefits, such as retirement income. As such, Social Security numbers are of little practical use to companies unless they are dealing with the government in some way. “Most of the time,” writes privacy advocate Chris Hibbert, “private organizations [such as businesses] that request your Social Security Number can get by quite well without your number.”³⁰ Nonetheless, Social Security numbers are used frequently enough as identifiers that many online retailers do ask for them—and many customers automatically provide them.

More Secretive Methods

Even when people do not have a customer relationship with a corporation—or do not knowingly provide much in the way of personal information—businesses can still harvest plenty of personal data about them. For example, it is common for retailers to track where a customer goes within the retailer’s website; but some businesses use software to monitor the other sites their customers visit as well. That can help the retailer flesh out a profile of the individual customer, enabling it to tailor its offerings more closely to the customer’s taste. This can be of some benefit to the customer. Still, to many web users, the procedure smacks of spying.

Manufacturers of technology often do the same. Apple, the manufacturer of the iPhone as well as various computers and tablets, is one example; the company keeps a record of what sites iPhone owners visit when they use their devices to go online. Some of these companies give customers the ability to opt out—that is, to refuse to allow the corporation to collect this type of information. But learning how to opt out can be tricky, and this is deliberate on the part of the company. As one writer says of Apple, instructions for how to opt out “are buried deep within the bowels of the iPhone, opaquely worded, and not located where you might

think they are.”³¹ The result is that many people give up looking, allowing Apple to continue to monitor which websites they visit.

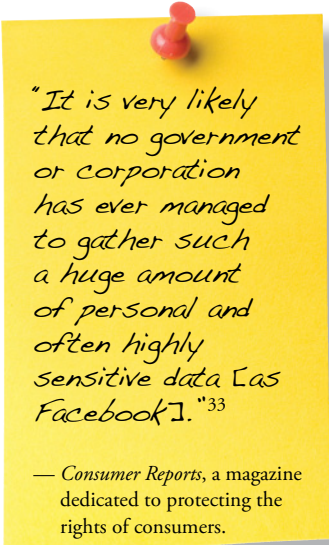
Other companies also collect data in unexpected and somewhat secretive ways. One of the champions of this practice is Facebook, a company that relies on users providing detailed information about their activities and lives. Facebook, however, goes further by capturing data from people who do not necessarily wish to share that information with the site—or who are not even members. “Facebook gets a report every time you visit a site with a Facebook ‘Like’ button,” explains the magazine *Consumer Reports*, “even if you never click the button, are not a Facebook user, or are not logged in [to Facebook].”³² This data might include the time

the page was visited, the exact location of the viewer at that moment, the length of time the viewer stayed at the site, and much more. “It is very likely that no government or corporation has ever managed to gather such a huge amount of personal and often highly sensitive data,”³³ says *Consumer Reports*.

How the information companies collect is used is another issue. Most corporations with an online presence offer so-called privacy policies; that is, they explain what data they collect from customers and what they do with it. Most consumers, however, ignore the policies altogether or approve them without a second thought—and often for good reason; they are long and frequently legalistic, making them hard to understand.

The complexity of some privacy policies is suggested by Scripps Networks Interactive, a media-related corporation, whose policy includes the following: “‘Websites’ includes sites hosted by one or more web servers {however accessed and/or used, whether via personal computers, mobile devices or otherwise (collectively, ‘Computer’)}. . . .”³⁴ Few people have the patience or energy to wade through thousands of words like these.

Moreover, customers often cannot imagine a situation in which their data would be useful other than in their own dealings with a company. If this is their opinion, however, they are wrong. In fact, companies make very good use of the information they collect.



“It is very likely that no government or corporation has ever managed to gather such a huge amount of personal and often highly sensitive data [as Facebook].”³³

— *Consumer Reports*, a magazine dedicated to protecting the rights of consumers.



Apple, for example, sells information collected from customers to other companies, which then produce advertisements tailored to the customer. For instance, someone who has visited lots of sports-related websites may get ads for baseball tickets, golf equipment, and books and films about soccer, while someone whose visits run more toward sites about animals may see messages from pet food companies or wildlife organizations. “Facebook’s entire business model is based on selling targeted advertising,”³⁵ asserts technology writer Andrew Couts. Thus, giving information to one company may result in a quite different company ending up with it—perhaps against the customer’s wishes or interests.

Facebook is a master at collecting information about its users and their lives. Simply by visiting a site having a Facebook “Like” button, even nonusers provide the company with information about how and where they shop.

The Government

While the data businesses collect worry privacy advocates, many of these advocates are much more concerned about the data collected by the government. The government, after all, has police powers, and that fact makes many privacy advocates uncomfortable. It is not difficult to imagine a government misusing this data to harass

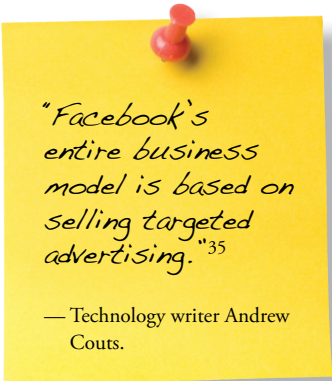
or even imprison its citizens. History, after all, is full of examples of countries that have done extensive spying on their people; Nazi Germany under Adolf Hitler and the Soviet Union under Josef Stalin are perhaps the best-known examples. The constitutional right to privacy seeks to avoid this type of situation by requiring that law enforcement may acquire information on people only if there is reason to believe that those people are up to no good. That provision is supposed to safeguard privacy rights against the power of the state, and in many, perhaps most, cases it is quite effective.

But in recent years the government has not always left innocent people alone. In 2001, in response to the terrorist attacks of September 11, Congress approved a bill known as the USA PATRIOT

Act. This law expanded the federal government's power to attack terrorism, particularly by relaxing some of the restrictions on law enforcement personnel. Recognizing that time could be of the essence when dealing with terrorist groups, the government took steps to streamline the process of gathering evidence and arresting people before they could carry out an attack. The act, for instance, made it easier for police forces to tap into phone calls without getting a warrant. The government was also given the right to search records of businesses—notably telecommunications companies, but other corporations

as well if authorities saw fit—without needing to inform the people whose records they were accessing.

The idea was to make it easier to find terrorists, especially those outside the country or those regularly communicating with foreigners. Former president George W. Bush, who signed the Patriot Act into law, was quite clear on this point. Soon after the passage of the act, Bush authorized the National Security Agency (NSA)—one of the government agencies responsible for gathering intelligence on enemies, including terrorists—to listen in on international phone calls and read international e-mails of people believed to have terrorist sympathies. Bush strongly emphasized the international nature of the program: “One end of the communication must be outside the United States,”³⁶ he directed. And most Americans, it is fair to say, support this kind of activity when



"Facebook's entire business model is based on selling targeted advertising."³⁵

— Technology writer Andrew Couts.



A protester in Atlanta, Georgia, expresses his opposition to domestic spying by the National Security Agency (NSA). Revelations that the NSA has been collecting e-mail, telephone, and other personal records of US citizens sparked an outcry in 2013.

it is specifically directed at people widely believed to be criminals or plotting to terrorize the United States. In 2011, for example, a survey found that 65 percent of Americans thought that the government should be allowed to monitor the e-mail and phone calls of “suspicious people.”³⁷ Even so, privacy advocates were alarmed that security forces would now be permitted to listen in on perfectly innocent calls to a business contact in Australia, a family member in Mexico, or a friend in France.

Moreover, the NSA did not limit its investigations to suspicious people following the passage of the Patriot Act. By 2006 there was evidence that the NSA had been collecting information on virtually every phone call made or received within the United States—whether to a foreign country or to another address in the same town. The government did not eavesdrop on these calls; instead, authorities collected basic information such as the locations

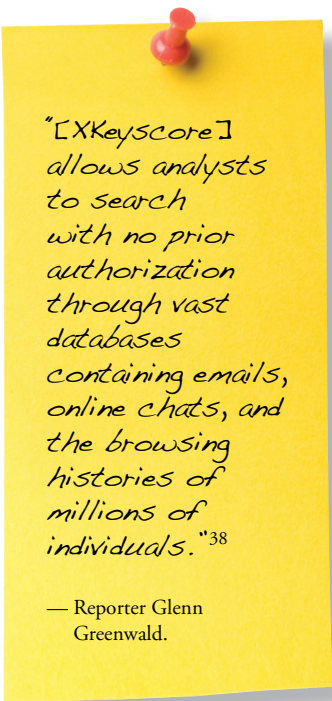
of the call's participants, the phone numbers involved, and the duration of the calls. But the great bulk of these calls involved people who were entirely innocent of any terrorist activity—and were not even suspected of any crimes. As with the warrantless wiretapping, the wholesale collection of data involving innocent people was of great concern to privacy advocates.

The XKeyscore Program

In one form or another, government programs that monitor Americans' activities continue to operate. In the summer of 2013, for example, information began appearing about a program called XKeyscore. This program had been used by the NSA for several years for the purpose of looking quickly through online data banks filled with the personal information of Americans. The program, according to journalist Glenn Greenwald, "allows analysts to search with no prior authorization through vast databases containing emails, online chats, and the browsing histories of millions of individuals."³⁸ XKeyscore also allows analysts access to Facebook messages and other social media sites. More than that,

federal agents can use this capability in a variety of ways. Not only can they track people by their phone numbers or e-mail addresses and check their online activity; they can also follow and investigate every person who visits a particular website or receives a given e-mail.

The goal of XKeyscore is the same as the goal of traditional spying and surveillance: to prevent crimes, especially terrorism. The main difference is that XKeyscore casts a much wider net; instead of looking only at those deemed suspicious, it looks at nearly everyone. The NSA argues that expanding its surveillance in this way has been successful. According to the agency, XKeyscore led to the capture of three hundred terrorists through 2008, with more criminals apprehended since then. At the same time, though, this success has come at a huge cost to privacy. The agency estimates that it collects up to 2 billion pieces of information every day through the use of XKeyscore. Much of this information relates to



"[XKeyscore] allows analysts to search with no prior authorization through vast databases containing emails, online chats, and the browsing histories of millions of individuals."³⁸

— Reporter Glenn Greenwald.

PRISM

In 2013 a National Security Agency (NSA) contract employee named Edward Snowden began leaking information to the general public about a secretive surveillance program called PRISM. Though PRISM was primarily a government program, it caught the attention of the public because it also relied on the cooperation of a number of private companies, most of them involved in technology and communication. Microsoft, for example, had been a part of the program since 2007, while Google and Facebook began taking part in 2009 and Apple joined in three years later.

PRISM collects an enormous amount of data involving Americans' communications. That may include monitoring videoconferences, looking at photos posted online, and determining when and where particular people log on to certain websites. The information is harvested originally by the companies, which are then required by a court order to hand it over to the NSA.

Snowden revealed the existence of the program in part, he said, because it showed that the government was far more involved in spying on Americans than most people knew. He also believed that much of the data collection was illegal. The government has disputed Snowden's characterization of the program, arguing that it is perfectly legal, carefully overseen, and much narrower in scope than Snowden believes. In June 2013 US prosecutors charged Snowden with espionage and theft of government property. Fearing for his safety, Snowden had already left the country; later that summer he was given temporary asylum in Russia.

people outside the United States, the agency is quick to add, and most of it is deleted after a day or two. Still, some of it surely relates to loyal and innocent Americans, and some of it remains on the record for an indefinite period.

The fact that innocent Americans' data is being accessed by the government is controversial. Though Americans tend to approve of electronic spying on people who have earned suspicion, they are less enthusiastic about spying on people who have not. A 2013 survey, for example, revealed that 52 percent of those surveyed believed that the government should not "monitor everyone's email to prevent possible terrorism."³⁹ There is no clear evidence that the data collected has been misused in any way or that the NSA and other organizations have actually violated the privacy of innocent citizens by releasing their names and information about them. Nonetheless, it is evident that programs like XKeyscore can potentially compromise the privacy of millions of Americans by allowing the federal government to collect sensitive personal data.

On the one hand, most Americans would agree that the right to privacy is important. On the other, most would also agree that the government needs to collect certain pieces of data in order to keep Americans safe from terrorism and other crimes. Unfortunately, the two goals of preserving privacy and fighting crime are at odds with each other. Requiring warrants helps safeguard privacy, but perhaps at the expense of allowing a terrorist attack that might have been thwarted with quicker action. Collecting information about every American's phone habits may help authorities find terrorists that they might otherwise have overlooked, but perhaps at the expense of privacy rights. Keeping the two in balance is a major challenge. Currently, as with business, the trend in government has been toward more and more data collection—with a corresponding infringement on the right to privacy.

Facts

- According to the research firm eMarketer, Americans spent about \$225 billion in online shopping in 2012.
- In a 2012 Pew Research Center survey, 68 percent of respondents had a negative opinion of targeted advertising.
- Some states forbid colleges from asking for students' Social Security numbers.
- According to the University of California Berkeley Center for Law and Technology, almost 98 percent of the most popular websites in the United States use cookies—software that tracks information about visitors.
- In 2001 the Patriot Act passed the House of Representatives by a margin of 357 to 66 and the Senate by a margin of 98 to 1.
- In a 2013 *Washington Post* survey, 48 percent of responders said they worried more about government going too far in investigating terrorism than about it not going far enough, with 41 percent disagreeing.

How Are Hackers Using the Internet to Violate Privacy?

In July 2013 New Jersey prosecutor Paul Fishman made an announcement of great interest to online security experts. Over the previous seven years, a group of criminals had successfully broken into the computer systems of a dozen or more American and European companies. From these endeavors, the thieves had made away with well over 100 million credit card numbers, each of them complete with the cardholder's name. Though at first there seemed to be few if any clues to the identity of the thieves, dogged detective work eventually led law enforcement officials to four Russian nationals and a Ukrainian. That July Fishman charged all five with having stolen the information. It was, Fishman said, the biggest "data breach scheme ever prosecuted in the United States."⁴⁰

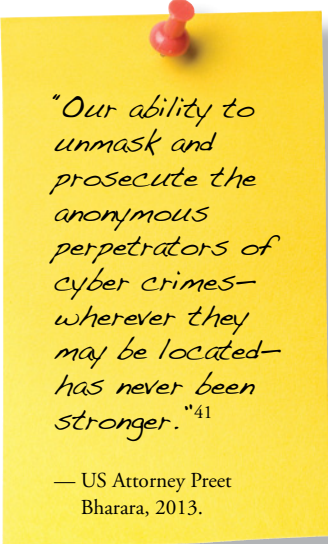
Simply announcing the indictments did not bring the case entirely to an end. Only two of the five conspirators were actually in police custody when the charges were handed down; the whereabouts of the Ukrainian and two of the Russians were unknown, and in their cases the indictment would have no effect as long as they remained at large. Moreover, an indictment is not the same as a conviction. As of August 2013 a trial was still to come, at which

any or all of the defendants could be found not guilty. Still, Fishman and other law enforcement personnel were sure they had the right men. “Our ability to unmask and prosecute the anonymous perpetrators of cyber crimes—wherever they may be located—has never been stronger,”⁴¹ said US Attorney Preet Bharara, who, like Fishman, believed that the five men were guilty as charged.

Breaching Security

Whoever committed the crimes knew what they were doing. The thieves targeted companies ranging from retailers such as 7-Eleven and JCPenney to the airline JetBlue, and at one point they managed to break into the records of NASDAQ, an electronic stock exchange. Their main focus, though, was on payment-processing companies. These businesses deal with credit card payments made to restaurants and other retailers. Some processors are very large: the hardest-hit company, Heartland Payment Systems of New Jersey, has more than one thousand employees and handles more than 100 million credit card payments each month. In most of these cases, the culprits remotely installed a piece of malware—malicious software designed to damage a computer system or take some control over it—on the companies’ computers. The malware secretly copied the credit card numbers as restaurants and other businesses sent them in, allowing the thieves access to the data.

The scheme did not manage to collect any further information from cardholders, such as birth dates, addresses, or Social Security numbers. Nonetheless, the security breaches had a major impact. Though Heartland Payment Systems and the other companies involved had taken steps to secure the personal data in their control to keep it safe from thieves, the thieves had circumvented these measures and demonstrated that the security systems were far from foolproof. Losses from the theft have been estimated at more than \$300 million, and it is not clear whether the companies involved will ever see that money again. Ordinary customers, even if they did not directly lose money, were inconvenienced by needing to



“Our ability to unmask and prosecute the anonymous perpetrators of cyber crimes—wherever they may be located—has never been stronger.”⁴¹

— US Attorney Preet Bharara, 2013.



JC Penney, which also goes by the name jcp, was among companies targeted by hackers in 2013. The hackers stole more than 100 million credit card numbers from about a dozen American and European companies.

get new credit card numbers; law enforcement personnel spent thousands of hours working on the case; and news of the theft pushed many members of the general public to wonder about the safety of their personal information online.

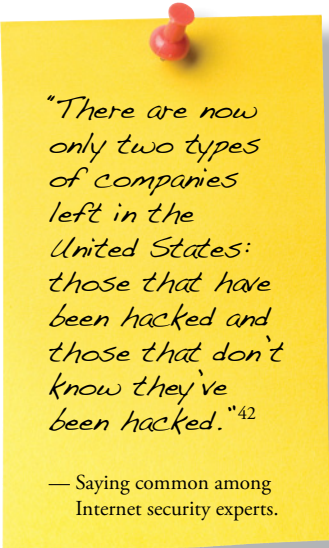
The Heartland case may have been the largest computer fraud case prosecuted in the United States to date, but it is certainly not the only one of its kind; nor, it is safe to say, will it be the last. On the contrary, gaining unauthorized access to computer systems and databases of both business and government has been an unavoidable consequence of the Internet age. This process, known informally as hacking, costs Americans tens of millions of dollars every year and compromises all manner of personal information, from birth dates to Social Security numbers. Because the data end up in the hands of thieves, moreover, hacking is of particular concern. Indeed, as some experts see it, of all the threats to privacy online, hacking is one of the most dangerous.

Early Hackers

Hacking is even older than the Internet. From the time computers became common in business and government, people have been trying to evade security systems and access the information the computers contain. As early as the mid-1970s, for example, two high school students in Chicago broke into their school's computer system and changed some of their grades. In 1982 a group of students in Milwaukee broke into the computer system at the Los Alamos National Laboratory in New Mexico, along with systems belonging to hospitals and other facilities. And in 1983 the movie *War Games* featured a fictional hacker who accesses a military supercomputer—and nearly starts a world war in the process. By 1986 the problem of hacking was significant enough that Congress had passed several laws specifically addressing it.

With a background like this, it is no wonder that the early days of the Internet included plenty of hacking efforts as well. In 1995 there were at least 250,000 separate illegal attempts to access computers at the US Department of Defense; more than half of these attempts were at least moderately successful. The following year hackers made unauthorized changes to the websites of a number of government agencies, among them the US Air Force, the US Department of Justice, and the Central Intelligence Agency. By 1998 three-quarters of government agencies, businesses, and nonprofit organizations with a web presence were reporting at least some hacker attacks. And in the following years the number only grew. Today hacking is so common that, as security experts like to put it, “there are now only two types of companies left in the United States: those that have been hacked and those that don’t know they’ve been hacked.”⁴²

Hackers have a variety of motivations for doing what they do. For some hackers, the goals of hacking are simply to challenge themselves and to have fun. Trying to gain unauthorized access to a website, for example, can be viewed as a test of a hacker's computer skills and creativity. Reformed hacker Kevin Mitnick,



“There are now only two types of companies left in the United States: those that have been hacked and those that don’t know they’ve been hacked.”⁴²

— Saying common among Internet security experts.

State-Sponsored Hacking

In some parts of the world, hacking—at least under some circumstances—is not only permitted but encouraged. Some countries have recruited computer-savvy people, especially young people, to hack for the government. In a twenty-first-century version of spying, these hackers spend their time trying to get into the computer systems of other nations, especially those with strong military capabilities, so they can steal classified information about weapons and tactics.

Nowhere is state-sponsored hacking more evident than in China. The United States is one of many countries that have accused the Chinese government of assigning hackers to try to break into top secret computer files. In May 2013, for example, US officials reported that Chinese hackers had successfully stolen data about twenty-five or more new weapons systems. At roughly the same time, Australia announced that hackers backed by China's government had accessed the plans for a building that would serve as Australia's spy headquarters. Earlier in 2013, similarly, another American report charged that hackers sponsored by the Chinese government had recently stolen information from as many as one hundred US companies. And in 2012, hackers from China made their way into the control systems of some of Canada's power grids.

China routinely denies playing any role, official or otherwise, in hacking. Indeed, authorities decry hacking as a threat to global security and insist that any Chinese hackers are acting on their own. The evidence gathered by military forces, corporations, and privacy experts in Australia, Canada, the United States, and other nations, however, strongly suggests otherwise.

now a computer security consultant, once said that his primary purpose in hacking was simply to “become better at getting in.”⁴³ Indeed, successfully attacking a corporate or government site may give hackers a certain status among their friends. In some cases hackers with this mindset see themselves as performing a public service by exposing flaws in security systems. “If we can share what we’ve learned with everybody and then publish it, that’s great,”⁴⁴ one hacker announced in an interview.

Another group of hackers is mainly interested in causing havoc. Like the hackers who changed government websites in the 1990s, these hackers hope to make life difficult for the owners of the sites they attack. “[They] simply enjoy destroying the work of others,”⁴⁵ sums up a website. People who hack for this reason are similar to graffiti artists who take pleasure in defacing walls or vandals who smash windows: they are engaged in destruction for its own sake, and the knowledge that someone else will have to clean up the mess makes them happy. Many of these hackers create and release viruses and other malicious software designed specifically to erase a computer’s memory, destroy valuable files, or otherwise interfere with the operation of a device. Computer viruses are effective, and fighting them takes time, effort, and money: According to one recent estimate, more than \$4.5 billion is spent each year dealing with the destruction caused by hackers who spread them.

Greed and Identity Theft

Probably the most common motivation for hacking is greed. Hacking can be quite lucrative. A successful attack on a website belonging to a corporation, government agency, or even an ordinary citizen can provide thieves with credit card numbers, birth dates, Social Security numbers, passwords, and more. This information can be extremely valuable. In the simplest situation, a thief can make online purchases with a stolen credit card number or cash withdrawals from an ATM using a debit card, especially when the card is attached to a person’s name and home address. Before the owner of the card realizes that it has been compromised, the thief may have purchased several thousand dollars’ worth of merchandise or completely drained a bank account. Though the

cardholder may not be responsible for most of the costs if the card can be shown to have been used fraudulently, the card companies lose money, the cardholder must spend time and energy fixing the problem, and the thief is the only one to come out ahead.

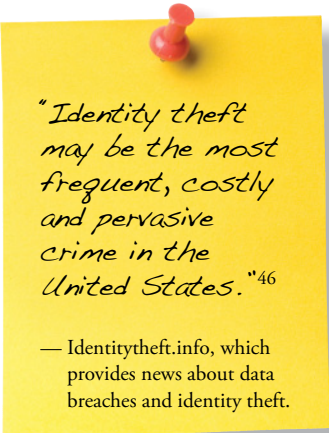
More sophisticated criminals use the information they steal as part of a larger scheme of identity theft. Criminals, often working in organized gangs, use stolen Social Security numbers, driver's license numbers, and other data to pretend to be someone else. They may take out loans or apply for new credit cards in the victim's name, using the victim's identifying information; because they have all correspondence sent to a different address, the victim may not know about the deception for months or even years. Of-

ten it is only when the victim applies for a loan and is turned down that the fraud becomes clear. According to one estimate, identity theft of this type is widespread, with one out of every fourteen American adults affected by it each year. As one expert puts it, "Identity theft may be the most frequent, costly and pervasive crime in the United States."⁴⁶

Not all hackers want to use stolen credit cards directly or take the time to build fraudulent identities. That is especially true in the case of large-scale hacking such as the kind that affected Heartland Payment Systems and 7-Eleven. Realistically, there was no way the thieves could use more than a tiny fraction of the hundreds of millions of data points that they collected. There is, however, a large online black market in credit card numbers and other pieces of personal information. Evidence produced in trials of Internet thieves suggests that a single valid credit card number, complete with card expiration date, security code, and owner's name, can be sold for about ten dollars. Nor is there any shortage of buyers for this information. One recent study located about fifty online "stores" trafficking in stolen financial data.

Anonymity

These practices are in one sense nothing new. Long before the Internet, thieves stole wallets and purses and used not only the cash



"Identity theft may be the most frequent, costly and pervasive crime in the United States."⁴⁶

— Identitytheft.info, which provides news about data breaches and identity theft.



Theft of personal items such as passports and wallets containing driver's licenses and credit cards is nothing new. What has changed, thanks to the Internet, is the speed with which thieves can operate and the expansive scope of what they can do with stolen personal information.

they found but the credit cards as well. In some cases, armed with driver's license numbers, passports, and other identifying information, resourceful thieves were able to steal an entire identity just as hackers do today—taking out loans, applying for credit cards, and even claiming the victim's Social Security benefits. Indeed, even today much identity theft has nothing to do with the online world. Instead, it begins with a purse snatching, an unshredded bank statement found in the trash, or an unscrupulous waiter who

illegally copies a diner's credit card information—just as it would have in the 1970s or 1980s.

But the Internet has made identity theft of all kinds far simpler. Most people whose purses or wallets are stolen become aware of the theft within hours, if not minutes, which limits the damage the thief can do. In an online world, though, the credit card itself remains safely in the owner's possession, and there are no immediate signs that the information has been compromised. Similarly, a pickpocket might come away with a handful of credit cards in an hour's work, while modern Internet thieves can pick up thousands of credit card numbers in the same time period. There is no way, for example, that the Heartland scam could have been perpetrated before the Internet. Even if the thieves could have gained access to the credit card numbers, they would have had no easy way to record and store them for later use.

At the same time, the anonymity of the Internet makes certain kinds of stolen information more valuable. When credit card transactions were mostly done in person or over the phone, a white male thief, say, would have a difficult time passing himself off as the African American woman whose driver's license and credit cards he had stolen. His skin color and gender would be immediate red flags, and even in ordering merchandise over the phone his masculine voice might be a giveaway. Today, in contrast, the same thief would have many fewer issues using the same stolen data. This makes identity theft more lucrative and less dangerous—and for both these reasons, more common.

Security Breaches

Indeed, every year there are dozens of online security breaches at companies and government offices alike. Some of these breaches have caused millions of pieces of data to be compromised. In 2011, for example, hackers exploited a vulnerability in Sony's online music and video service to carry out what Sony officials called a "very professional, highly sophisticated attack."⁴⁷ The thieves came away with extensive personal information about Sony customers, including the birth dates and mothers' maiden names (frequently used as a test question to prove identity) of more than 24 million



people. The hackers also harvested about twenty-three thousand credit and debit card records. Though Sony claimed that the records were encrypted and so would be of no use to the thieves, not all security experts agreed. In any case the incident unnerved many customers and caused a major public relations problem for Sony.

Other companies and agencies have been hit nearly as hard in the past few years. The member database for the social networking site LinkedIn, for example, was hacked in June 2012, with the hackers stealing millions of user passwords. The same year, hackers broke into the records of online shoe retailer Zappos and came away with customers' passwords, most of them encrypted, as well as phone numbers, e-mail addresses, and partial credit card numbers. The security breach at Zappos was not noticed until the hacker went online and asked for help decoding the encrypted passwords. And in 2011 the University of Connecticut informed people who had purchased school-themed items online that hack-

The University of Connecticut was hit by hackers in 2011. Hackers stole purchasing information (including credit card numbers and security codes) for school-themed items sold to buyers online.

ers had stolen much of their data—including many credit card numbers, along with the cards' security codes and expiration dates.

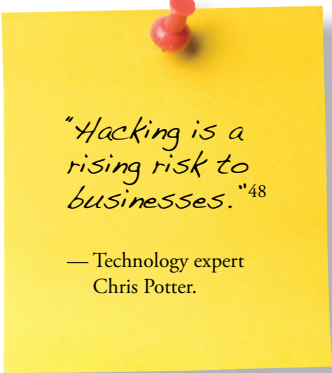
Some observers say, moreover, that the worst is yet to come. "Hacking is a rising risk to businesses,"⁴⁸ says technology expert Chris Potter. Certainly many companies and government agencies,

ranging from Google to the Los Angeles Police Department, have reported an upswing in hacking attempts over the past several years. One reason for the increase is that hacking has become a worldwide problem. A recent survey of companies that admitted to being hacked revealed that 30 percent of the attacks come from hackers in China, with nearly as many coming from Romania. The United States has no jurisdiction to arrest hackers in other countries, and the governments of some nations show little inclination to police hackers' activities. In

early 2013, for instance, the United States demanded that China take steps to end its citizens' hacking of American computer networks; whether that will have any effect remains to be seen.

The Future

Another reason for the surge in hacking attempts has to do with security flaws. Not every company uses state-of-the-art security to protect itself from being attacked. In a recent survey, one company in every five devotes less than 1 percent of its information technology budget to securing its data. "Scrimping and saving on security creates a false economy,"⁴⁹ says Potter, who points out that the cost of fixing a security breach is likely to be much greater than the cost of establishing a secure network to begin with. Wyndham Hotels, whose database was hacked in 2008, is a prime example. "Wyndham failed to use industry-wide best practices such as using complex passwords and user IDs," explains one website; this failure made it easy for hackers to enter the system. And after Wyndham officials discovered what was going on, the website continues, "they did not make changes to their security procedures and the hacking continued for years."⁵⁰ When large companies are not taking the proper steps to ward off cyberattacks, there is little incentive for hackers to stop their activities.



*"Hacking is a
rising risk to
businesses."⁴⁸*

— Technology expert
Chris Potter.

Phishing and Keylogging

Though many hackers focus their attention on getting access to the computer systems of large businesses and governments, some try to attack individual people's personal computers instead. Two common methods they use are phishing and keylogging.

Phishing involves sending fake e-mail messages purporting to be from banks or other online businesses. These messages may tell people that their payments are delinquent or that their accounts have been deactivated; they include a link to a website, supposedly the company's, where the customer can go to resolve the situation. The link, however, goes to a website unaffiliated with the legitimate business. The customer is prompted to type in account numbers, passwords, and other sensitive information, which is then read by the scammers. To combat phishing, most experts advise calling the company to see if the e-mail is legitimate, typing the web address of the business into the browser rather than using the link provided, or simply deleting the e-mail altogether.

In keylogging, hackers install special software on a computer that tracks the keystrokes the computer's user makes. "In no time the hacker will have the usernames and passphrases for a number of your online accounts," writes author Matthew Bailey. The software can be installed in person, with a physical device attached directly to the computer; it can also be installed remotely, usually via a computer virus. To reduce the risk of a virtual keylogging program, experts recommend never clicking on any e-mail attachment from an unknown source.

Matthew Bailey, *Complete Guide to Internet Privacy, Anonymity, & Security*. Nerel, 2011, p. 29.

Other reasons can also explain why hacking is becoming more and more common. There is a stigma about reporting a security breach, for example, that leads some companies to avoid publicizing what happened—making it more likely that the hackers will escape prosecution. Similarly, investigating security breaches is difficult and complex and requires specialized knowledge, again making it difficult to track down the perpetrators of any given hacking incident. But the main reason that hacking is becoming steadily more popular is simply that the reward is so high. If a single cyberattack nets a hacker, say, one thousand credit card numbers, the hacker can sell the numbers on the black market for about \$10,000—a significant payoff. And the more information a person can gather, the higher the reward.

But though hackers may benefit from their activities, the economy and the general public certainly do not. Hackers, after all, are fundamentally thieves: they make away with money and information that belongs to others. Since 2005, according to one estimate, the total cost associated with data breaches is approximately \$200 billion. Beyond cost, though, the prevalence of hacking in the modern world has been highly invasive of personal privacy. In the last few years alone, millions of Americans have been notified that their personal information has been compromised and perhaps stolen because of a cyberattack on a business or a government agency. If hacking does indeed become an even greater problem in the future, this will make the threat to personal data that much stronger. Whether or not their information has already been stolen in this way, hacking should concern all Americans.

Facts

- One of the first federal laws to address hacking was the Computer Fraud and Abuse Act, passed in 1986.
- In December 2012 hackers stole the Social Security numbers of thirty-six thousand people who visited a military base, including the numbers of many intelligence officers.
- According to the US Bureau of Justice Statistics, identity theft cost American households more than \$13 billion in 2010.
- The US Department of Homeland Security is largely responsible for protecting the US government's information technology system from hacking.
- As of 2012 only 65 percent of North American businesses used software to protect their computer systems from malware and viruses.

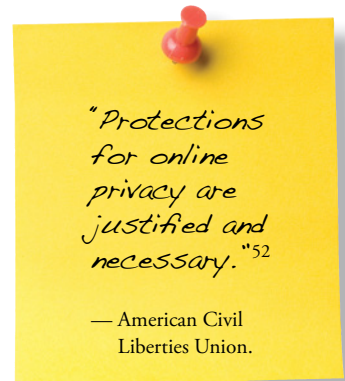
What Can Be Done to Limit Privacy Violation on the Internet?

Most Americans argue that the Internet has eroded personal privacy, and most Internet security experts would agree. The sheer number of databases accessible on the Internet, the cautionary stories of websites hacked and information stolen, the all-too-common instances of cyberbullying—each of these strongly suggests that privacy is becoming more and more difficult to safeguard online. Even people who maintain a minimal Internet presence still have a great deal of personal information stored on the web. Staying away from social media sites, rarely surfing the web, and never paying bills online cannot guarantee that personal data will remain personal. The advantages of storing information electronically make it practically impossible to avoid some infringement of privacy in the modern world.

But while there is not much debate over whether privacy is being eroded by the Internet, there is much more debate about the importance of this change. For some observers, privacy is over-

rated. As they see it, whatever privacy people once had no longer does or should apply to a modern and increasingly wired world. “Privacy is dead—get over it,”⁵¹ announced private investigator Steve Rambam at a 2006 conference. This perspective has been echoed many times in recent years, particularly by people who work in the technology industry. Facebook founder Mark Zuckerberg and onetime Sun Microsystems CEO Scott McNealy, just to name two, have made statements similar to Rambam’s over the past decade and a half. In this view, there is no point in trying to safeguard privacy rights; the battle is over, and the forces supporting privacy rights have lost.

Many other Americans, however, are not quite so willing to give up the fight. To them, the increasing loss of privacy is a serious problem and one that must be stopped if at all possible. “You shouldn’t have to choose between using . . . technology and keeping control of your private information,” argues the American Civil Liberties Union (ACLU), an advocacy group concerned with the preservation of basic rights. “Protections for online privacy are justified and necessary.”⁵² In most surveys, Americans agree with this perspective; in a 2013 survey, nearly three-fourths of respondents agreed that online privacy rights were important. To what extent privacy rights can be strengthened is uncertain, but promoters for greater privacy protections have suggested a number of possible avenues, from personal decisions to laws, that may help buttress the rights that exist today.



Individual Action

Strengthening privacy online, in many cases, starts with individuals. There are many options for controlling the degree to which technology users put their privacy at risk online. One common piece of advice, for example, is to choose passwords for e-mail, purchasing accounts, and social networking sites that cannot be easily compromised. “Your information is only as secure as the passphrases you use to protect it,” warns author Matthew Bailey. Like other experts, Bailey suggests using passwords that are more than six or seven characters long, contain numbers and symbols (such as * or



High school and college students are more likely to post online personal details and photos that do not belong in the public domain. Reckless behavior online, experts say, can have ramifications both immediate and long term.

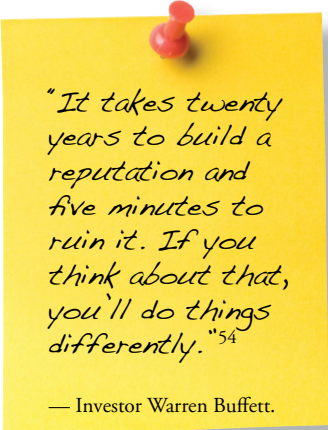
%), and include no recognizable words or personal information such as birth dates. “Pick something random and even ridiculous,” Bailey advises, pointing out that if a password is too difficult to identify, prospective hackers “will move on to an easier victim.”⁵³

Password protection is especially important for two reasons. The first is the tendency for people to use the same password, or the same password with small variations, at multiple sites. Thus, a hacker who determines the password for a person’s online gaming account may also be able to use the same password to access the owner’s bank account. The first is an annoyance; the second is an enormous problem. Second, even if the passwords are different, a hacker who gains access to a person’s e-mail account may very well be able to find passwords for other accounts in the stored e-mails. Most people have at one point or another forgotten various passwords and requested that they be re-sent. That information is therefore available to anyone who manages to hack into the e-mail—a

task that is a lot simpler if the account's owner uses a weak password.

Another way in which people can protect their privacy online has to do with what they post on social networking sites. Most experts advise being extremely cautious about the kind of information posted. It is always a bad idea to post personal information such as birth date, home address, or vacation plans, as these pieces of data could be used to steal a person's identity or to plan a burglary. Perhaps even more important is the need to post thoughtfully. A complaint about an employer could cause termination from a job if a boss happens to see it. Controversial pictures, posts, and tweets can break up marriages, void a security clearance, or cancel a job offer. Accordingly, experts strongly suggest that people think before they post. As investor Warren Buffett says, "It takes twenty years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."⁵⁴

Efforts to convince people not to post sensitive information tend to be directed toward high school and college students. Evidence shows that teenagers and young adults are more likely than older people to post highly personal details about themselves online. They are also more likely to post pictures of themselves or accounts of their activities that may disqualify them from jobs with companies that look closely at a job applicant's Internet presence—more than half of all employers and growing, according to a 2011 study. The somewhat reckless posting makes sense; due in part to their brain chemistry, people in this age group are more likely to take risks and have a more difficult time thinking ahead than people who are older. Thus, schools are increasingly taking an active role in reminding their students of the consequences of misusing social media. A company called Human Relations Media, for example, offers a DVD for school use titled *Me and My 500 "Friends": Staying Safe on Social Networks*.



"It takes twenty years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."⁵⁴

— Investor Warren Buffett.

Posts About Others

Unfortunately, in today's social media-heavy world, it is not always possible to prevent potentially sensitive pictures or information from being posted by other people. There is nothing to prevent a

Reputation Management

One form of privacy infringement has to do with negative information about a person posted on the Internet. Negative information can be quite common; it may result from negative feedback on business transactions, or it could happen because of various forms of online harassment. In either case it can be embarrassing for a person to do a search for his or her name and see mainly negative information come up.

A number of companies advertise that they can remedy this situation. Known as reputation management companies, they use a variety of methods. It is possible, for example, to put positive information online about the person by publishing new social media profiles or blogs that mention his or her name. When someone uses a search engine to look for the person in question, some of these sites may displace some of the negative sites at the top of the list of results. If people believe that the negative information posted against them is not true, the reputation management company may politely but firmly request that the information be taken down—or threaten a lawsuit if this request is not followed.

These are all widely considered to be ethical ways of reestablishing a good reputation on the Internet. But according to Michael Fertik, founder of one of the best-known reputation management companies, not all of these companies behave ethically. Some, for example, may try to damage the offending websites by infecting them with malware or a computer virus in hopes that the websites will be shut down.

person from snapping a picture of a friend, posting the picture on Facebook or a similar site, and then “tagging” the picture with the friend’s name. If the picture might be offensive or embarrassing,

there is nothing the subject can do about it—except ask politely that it be taken down as quickly as possible. The best advice in this case is for people to let their friends know that they do not wish to have their images or names appear on the web at all. Even the most security-conscious experts acknowledge, however, that this can be difficult—especially for teenagers and young adults, for whom social media is very commonly the main form of communication.

Internet bullying is another matter. Online harassment is not just an invasion of privacy; it is also undeniably cruel. Over the past decade or so, there has been a growing chorus for laws that can perhaps prevent or limit cyberbullying, or at least establish significant penalties for those who engage in it. The outcry against cyberbullying took shape in 2006, when a thirteen-year-old Missouri girl named Megan Meier committed suicide after a particularly egregious incident of cyberbullying. Meier's middle-aged neighbor, Lori Drew, had set up an online profile for a fictitious sixteen-year-old boy named Josh. Using that profile, Drew befriended Meier online, flirted with her for a time, and then abruptly turned on Meier and dropped her as a friend. "The world would be a better place without you,"⁵⁵ Drew had Josh tell Meier; and Meier, who had a long history of depression, killed herself later that day. At the time, neither Missouri nor the federal government had any specific laws against cyberbullying, so Drew was convicted only of computer fraud related to her invention of Josh—a conviction that was later overturned.

Many people, however, were appalled that Drew had escaped any penalty for her actions, and in the wake of the incident various governments began passing laws that dealt specifically with cyberbullying. Missouri's law, for instance, applies to people who cause emotional distress "by anonymously making a telephone call or any electronic communication"⁵⁶ and—in a clear nod to the Meier case—calls for stricter penalties if the harassment is committed by a person over twenty-one against a person younger than eighteen. These laws have not been universally popular; some worry that the legislation is written too broadly and may infringe on free speech. (Indeed, parts of Missouri's law were overturned by the state Supreme Court on exactly these grounds.) The existing

laws, however, may help curb some of the worst excesses of online harassment. If nothing else, the increasing awareness of the harm cyberbullying causes may help reduce its prevalence in the future.

Limits on Business

Just as some legislators have sought to solve the problem of cyber-harassment by criminalizing it, so too have some lawmakers tried to pass laws to control the amount of information businesses can collect. Many of these efforts have focused on preventing companies from gathering information from children. In 1998, for example, the Federal Trade Commission, an arm of the federal government, introduced the Children Online Privacy Protection Act, also known as COPPA. This law covers companies that market to children, defined in this case as those below age thirteen. It states that companies that run websites aimed at children must make it clear what information they are seeking and how it will be used; more important, it requires that a parent formally approve the collection of any information. As the act puts it, these companies must “obtain verifiable parental consent”⁵⁷ in order to gather any of this data. Most experts agree that COPPA and similar laws have been reasonably effective in limiting what corporations can find out about children.

Legal restrictions on what data companies can collect from adults, however, are much less common. While many corporations that do business online have privacy policies that specify what information they collect from customers and how it will be used, no federal laws mandate these policies. Moreover, only a few states have legislation relating to privacy policies. Connecticut is one of the few that mandates any kind of privacy policy, but its law applies only to those companies that collect Social Security numbers. Among other restrictions, the law requires companies doing business with Connecticut customers online to “protect the confidentiality of Social Security numbers [and] prohibit unlawful disclosure”⁵⁸ of them. However, the penalties for violating this law are not especially stiff. Not only can companies evade any punishment at all simply by claiming that failing to provide a privacy policy was unintentional, but the fine for knowingly breaking the law is just \$500 per customer.



A few other states have laws that deal with privacy online in other ways. Though Nebraska does not require companies to publish a privacy policy, for example, it does insist that any privacy policies be accurate. As part of an effort to prevent deceptive trade practices, state law prohibits “knowingly making a false or misleading statement in a privacy policy . . . regarding the use of personal information submitted by members of the public.”⁵⁹ Minnesota and Nevada require Internet service providers to keep their customers’ personal information private, unless the customer agrees that the providers can share the information. Such laws are relatively rare, however; the bulk of states have no similar protections for customers.

Some states have passed laws that aim to protect the online privacy of consumers and employees. In Illinois, for instance, employers may not require employees or job applicants to share their social media passwords during job interviews.

Effectiveness of Laws

Somewhat more common are prohibitions regarding what employers may know about their employees’ online activities. Delaware, for example, specifies that employers must warn their em-

State Laws and Privacy

Relatively few states have passed laws protecting privacy on the Internet. One reason for this is the nature of modern business. Virtually any company with an online presence does business in all fifty states and very often in all the provinces of Canada as well. Many also conduct transactions in Asia, Europe, and elsewhere.

For these companies, trying to keep up with all the laws that pertain to each of these places is already extremely difficult; adding privacy laws into the mix would make the situation even more complicated. That is especially true if the laws were not exactly the same, as is usually the case with laws passed at different times by different states. If one state required companies to issue a privacy policy with specific wording and another state mandated a privacy policy with different language, the complexity would increase even more.

This is one reason why many people believe the only way to safeguard Internet privacy through legal means is to pass laws at the federal level, which would cover all the states and territories at once. If it could be passed, such a law would cover the entire population of the United States, making it much simpler for businesses to follow. Because of lobbying by businesses and little sense of urgency on the part of the public, though, federal laws governing Internet privacy have yet to be passed.

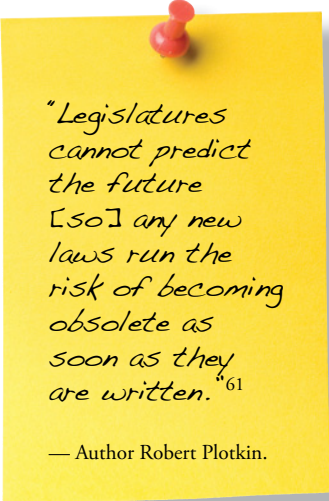
employees if they decide to monitor workers' e-mails and Internet usage while at work. This does not by any means prevent employers from checking up on their employees' online activities, but it does serve to alert workers that their online presence may not be completely private. Other laws relate to employer demands for access to employees' personal postings on social media sites. Some businesses argue that they need to monitor these postings to make

sure proprietary information is not leaked, but a number of states have recently passed laws banning or severely restricting the practice. An Illinois law approved in 2012, for instance, makes it illegal for employers even to ask for a social networking password, let alone to require it as a condition of employment.

Still, most states have very little legislation that safeguards online privacy. Some Internet experts argue that more laws would be helpful in protecting privacy rights. The ACLU, for example, strongly urges the passing of new legislation that would limit the amount of data corporations could collect and make the process of collection, when it occurs, more apparent so that customers could more easily choose not to let their data be harvested. “It’s time for new privacy laws,”⁶⁰ the ACLU argues, pointing out that going online should not automatically mean sacrificing personal data and privacy.

The degree to which laws can successfully protect privacy, however, is debatable. Some observers assert that given the pace of technological change, adding new laws is not very helpful. “Legislatures cannot predict the future,” author Robert Plotkin points out. Thus, he notes, “any new laws run the risk of becoming obsolete as soon as they are written.”⁶¹ Other experts believe that there are too many obstacles to passing effective laws—obstacles that include unwilling legislators, an often apathetic public, and powerful businesses that do not wish to limit the information they can collect. Despite the polls that show support for online privacy laws, states and the federal government have been more likely to reject this type of legislation than to approve it. “The public has not been good about demanding privacy laws,” notes journalist Adam Cohen; moreover, he adds, “industry has been very good at blocking them.”⁶²

As a result, many people believe that mandating specific laws for businesses is not the best way to safeguard Internet privacy. Instead, they argue in favor of voluntary guidelines. In this model, corporations would work together to draw up codes of conduct for each industry. Though government would not require any corpo-



“Legislatures cannot predict the future [so] any new laws run the risk of becoming obsolete as soon as they are written.”⁶¹

— Author Robert Plotkin.

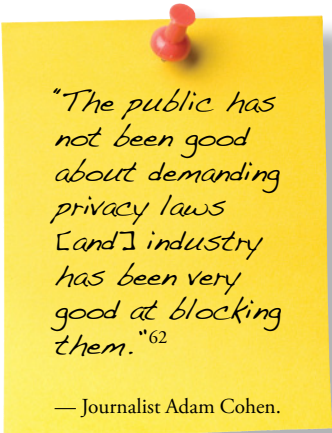
rations to follow these guidelines, the hope—and expectation—is that most reputable businesses would agree to do so. The privacy policies would be clearly stated and easy to find on each company's website. With an industry-wide standard, consumers would know exactly what information was being collected and how it would be used wherever they went on the web. The US Department of Commerce, among other organizations, has championed the idea of voluntary codes of conduct, which may indeed prove helpful if they are instituted.

The Government

Keeping personal information safe from the government is a similar issue, but because of the nature of government, it is considerably more nuanced. While stores and other businesses may have no good reason to ask for customers' birth dates or Social Security numbers, this information is vital for at least some government agencies. It is therefore more difficult to justify putting limits on what information governments may collect about individuals. On the other hand, governments have powers that businesses do not.

In particular, governments have police powers: They can put people in prison based on the private information they gather, but businesses do not have that authority. From this perspective, it is all the more vital to keep governments from getting unnecessary and sensitive information about its citizens.

As with businesses, some states have passed laws limiting what government may know about its citizens—and how it may use that information. While hardly any states mandate privacy policies for businesses on the Internet, about a third of the states have similar legislation requiring government sites to post privacy policies. As the law for Maine reads, "Each public entity that has a publicly accessible site on the Internet associated with it shall develop a policy regarding its practices relating to personal information and shall post notice of these practices on its publicly accessible site."⁶² Other states provide slightly different protections. According to Arizona law, for example, public libraries may not reveal patrons'



"The public has not been good about demanding privacy laws [and] industry has been very good at blocking them."⁶²

— Journalist Adam Cohen.



Public libraries have long sought to keep patrons' records private. In Arizona, a law forbids libraries from providing patrons' records to police.

records to police. And on a national level, a bill under consideration by Congress in the summer of 2013 would require the federal government to obtain warrants in order to access most e-mails sent to or by Americans.

Again, whether legal remedies will prove sufficient to protect privacy rights online from the government is unclear. While there may be more enthusiasm for restricting what data the government can gather than for restricting what businesses may collect, the fact remains that as of 2013 two-thirds of the states do not even require government agencies to post privacy policies on their websites. Nor do they restrict government access to e-mails, prevent

the government from collecting unnecessary information, or limit what the government may do with the data it harvests. This is not to say that governments routinely misuse the information they collect; in most cases they do not. But the possibility is there, and most governments have not taken many steps to tighten the restrictions. Until and unless that takes place, it will be all too easy for governments at all levels to violate privacy rights.

Personal Responsibility

In the end, the question of preserving privacy online comes down to the will of the American people. For the most part, despite their stated concerns about privacy violations, Americans have done little to stop the erosion of privacy through the Internet. Not only do many people casually post potentially compromising information about themselves, but many others do not take even basic steps to protect their data from hackers. More significantly, Americans tend to give businesses and governments the personal information they request without asking whether the data is necessary or how it will be used.

And while a few organizations, notably the ACLU, work to keep questions of online privacy in the minds of Americans, the public has not generally showed much interest in pushing legislatures to pass laws regulating the gathering of information—or even to establish voluntary codes of conduct for corporations that collect private data. In the end, if privacy rights online are to be safeguarded, it will be necessary for Americans to become less apathetic about keeping their personal information to themselves.

Facts

- According to SplashData, the most common passwords in the United States include *password*, *12345678*, and *abc123*—all of which are very easy for hackers to guess.
- About 10 percent of teenagers say they have been victimized by someone who has taken a picture of them and circulated it on social media without consent, according to a Pew report.
- As of July 2013 the only state without any kind of law against bullying was Montana. Nearly all other states specifically include cyberbullying or electronic harassment within their anti-bullying laws.
- To avoid having to deal with the provisions of COPPA, many websites—including social media sites like Facebook—bar people under age thirteen from using their sites.
- According to researchers at Carnegie Mellon University, it would take seventy-six work days for a typical American to read through all the privacy policies he or she encounters in a year.

Source Notes

Introduction: Privacy and the Right to Know

1. Quoted in Rebecca Shapiro, “New York *Journal News* Publishes Gun Owners’ Names in Westchester, Rockland Counties,” *Huffington Post*, December 26, 2012. www.huffingtonpost.com.
2. Quoted in Shapiro, “New York *Journal News* Publishes Gun Owners’ Names in Westchester, Rockland Counties.”
3. Quoted in Christine Haughney, “After Pinpointing Gun Owners, Paper Is a Target,” *New York Times*, January 6, 2013. www.nytimes.com.
4. Scott Robertson, “Privacy Is Dead—Deal with It,” *Ragan’s PR Daily* (blog), January 16, 2013, Document1www.prdaily.com.

Chapter One: What Are the Origins of the Internet Privacy Controversy?

5. US Constitution, Second Amendment.
6. US Constitution, Fourth Amendment.
7. Quoted in Milton R. Konvitz, *Fundamental Rights*, New Brunswick, NJ: Transaction, p. 112.
8. US Constitution, Fourth Amendment.
9. *Katz v. United States*, 389 U.S. 347, December 18, 1967.
10. Quoted in RT, “Cell Phone Users ‘Have No Legitimate Expectation of Privacy’—Judge,” May 17, 2013. <http://rt.com>.
11. The Cajun Boy, “What Would Life Be like in a World Without the Internet?,” *UPROXX: The Culture of What’s Buzzing* (blog), March 21, 2013. Document1www.uproxx.com.
12. Quoted in Debra Cassens Weiss, “School Used Student’s Facebook Photo to Illustrate How Embarrassing Posts Never Die, Suit Says,” *ABA Journal Blawg*, July 8, 2013. Document1www.abajournal.com.

Chapter Two: What Is the Effect of Social Media on Privacy?

13. Pinterest, “About,” 2013. <http://about.pinterest.com>.

14. Kenneth Wisniewski, "Like It or Not, Social Media Has Changed Our Society," *Ken Wisniewski's Blog* on *Webimax* (blog), May 20, 2013. www.webimax.com.
15. Mike Giglio, "The Cyberactivists Who Helped Topple a Dictator," *Daily Beast*, January 15, 2011. www.thedailybeast.com.
16. Quoted in Robert Plotkin, *Privacy, Security, and Cyberspace*. New York: Facts On File, 2012, p. 102.
17. Quoted in Marshall Jones Jr., "Tips for Creating Fresh Twitter Content," *Marshalllogue* (blog). <http://marshalljonesjr.com>.
18. Jon Green, "We Don't Need Facebook to Violate Our Privacy; We Do It to Ourselves," *Americablog*, November 28, 2012. <http://americablog.com>.
19. Green, "We Don't Need Facebook to Violate Our Privacy; We Do It to Ourselves."
20. Quoted in Twitter, "Please Quit Posting Pictures of Your Debit Card, People," June 20, 2013. <https://twitter.com>.
21. Quoted in RT, "Facebook Users Risk Identity Theft," March 21, 2013. <http://rt.com>.
22. Carah Friedman, "What Identity Thieves Can Learn from Your Online Profile," in *Jerry D. Russell.com* (blog), July 8, 2013. <http://jerrydrussell.com>.
23. Quoted in Tara Moore, "Privacy Expert Uses Online Photos to Predict Social Security Numbers," *CIT Magazine*, Winter 2011–2012. www.cit.cmu.edu.
24. Quoted in Leanne Italie, "Divorce Lawyers: Facebook Tops in Online Evidence in Court," *USA Today*, June 29, 2010. <http://usatoday30.usatoday.com>.
25. Billie Hara, "Think Before You Tweet (or Blog or Update a Status)," *Chronicle of Higher Education* "Blogs," February 23, 2011. <http://chronicle.com/blogs>.
26. Quoted in *Maclean's*, "10 Years Later, 'Star Wars Kid' Speaks Out," May 9, 2013. www2.macleans.ca.
27. Quoted in Lindsey Riley, "Cyber Bullying Affects Adults, Too," KVAL News, October 4, 2012. www.kval.com.

Chapter Three: How Is Data Collection Undermining Privacy on the Internet?

28. Randall Munroe, "The Problem with Wikipedia," *xkcd*. <http://xkcd.com>.

29. Sears, e-mail correspondence, "Thank you for your purchase!," April 12, 2012.
30. Chris Hibbert, "SSN FAQ: Private Requests for Your SSN," Computer Professionals for Social Responsibility, March 3, 2001. <http://cpsr.org>.
31. Jason Gilbert, "iPhone Privacy: How to Stop Apple and Advertisers from Tracking You on iOS 6," *Huffington Post*, October 15, 2012. www.huffingtonpost.com.
32. *Consumer Reports* staff, "Facebook and Your Privacy," Yahoo! Finance, May 3, 2012. <http://finance.yahoo.com>.
33. Quoted in *Consumer Reports* staff, "Facebook and Your Privacy."
34. Scripps Network Interactive, "Privacy Policy," 2013. www.scrippsnetworksinteractive.com.
35. Andrew Coutts, "State of the Web: Who Killed Privacy? You Did," Digital Trends, August 7, 2012. www.digitaltrends.com.
36. Quoted in Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," *USA Today*, May 11, 2008. <http://usatoday30.usatoday.com>.
37. Quoted in John Dickerson, "Why Americans Don't Fear the NSA," *Slate*, June 7, 2013. www.slate.com.
38. Glenn Greenwald, "XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet,'" *Guardian* (London), July 31, 2013. www.theguardian.com.
39. Quoted in Pew Research, "Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic," June 10, 2013. www.people-press.org.

Chapter Four: How Are Hackers Using the Internet to Violate Privacy?

40. Quoted in Associated Press, "US Attorney in NJ Announces Largest Alleged Hacking, Data Breach Scheme Ever Prosecuted in US," Fox News, July 25, 2013. www.foxnews.com.
41. Quoted CBS New York News, "Officials: 5 Charged in Largest Hacking, Data Breach Scheme Ever Prosecuted," July 25, 2013. <http://newyork.cbslocal.com>.
42. Nicole Perlroth, "The Year in Hacking, by the Numbers," *Bits* (blog), *New York Times*, April 22, 2013. <http://bits.blogs.nytimes.com>.
43. Quoted in Plotkin, *Privacy, Security, and Cyberspace*, p. 55.
44. Quoted in Online *NewsHour*, "Hacker Profile," PBS. www.pbs.org.

45. *TechNet* (blog), Microsoft, “Motivations of a Criminal Hacker,” 2013. <http://technet.microsoft.com>.
46. IdentityTheft.info, “Identity Theft Victim Statistics,” 2012. www.identitytheft.info.
47. Quoted in Julianne Pepitone, “Massive Hack Blows Crater in Sony Brand,” CNN Money, May 10, 2011. <http://money.cnn.com>.
48. Quoted in Nick Mann, “Hacking on the Increase, Says PwC,” *Actuary*, April 26, 2012. www.theactuary.com.
49. Quoted in Mann, “Hacking on the Increase, Says PwC.”
50. *Symform* (blog), “5 Worst Cyber Security Breaches of 2012.” www.symform.com.

Chapter Five: What Can Be Done to Limit Privacy Violation on the Internet?

51. Quoted in Coutts, “State of the Web.”
52. American Civil Liberties Union, “Internet Privacy.” www.aclu.org.
53. Matthew Bailey, *Complete Guide to Internet Privacy, Anonymity, and Security*. N.p.: Nerel, 2011, p. 23.
54. Quoted in Plotkin, *Privacy, Security, and Cyberspace*, p. 62.
55. Quoted in Jennifer Steinhauer, “Verdict in MySpace Suicide Case,” *New York Times*, November 26, 2008. www.nytimes.com.
56. Missouri General Assembly, “Missouri Revised Statutes,” August 28, 2012. www.moga.mo.gov.
57. COPPA—Children’s Online Privacy Protection Act of 1998, “Title XIII—Children’s Online Privacy Protection,” www.coppa.org.
58. Connecticut General Assembly, “An Act Concerning the Confidentiality of Social Security Numbers,” Connecticut Laws. www.cga.ct.gov.
59. Nebraska Legislature, “Nebraska Revised Statute 87-302.” <http://uniweb.legislature.ne.gov>.
60. American Civil Liberties Union, “Internet Privacy.”
61. Plotkin, *Privacy, Security, and Cyberspace*, p. 13.
62. Adam Cohen, “Internet Privacy: A New Bill Finally Offers Protections,” *Time*, April 30, 2013. <http://ideas.time.com>.
63. Maine State Legislature, “Maine Revised Statutes.” www.mainelegislature.org.

Related Organizations and Websites

Association for Competitive Technology

1401 K St. NW, Suite 502
Washington, DC 20005
phone: (202) 331-2130
website: <http://actonline.org>

This international organization is an association of information technology businesses. It lobbies on behalf of its members and encourages innovation in business and technology. It is often reluctant to support laws that strengthen privacy rights because of fears that such laws will disrupt commerce and limit consumer choices.

Electronic Frontier Foundation

815 Eddy St.
San Francisco, CA 94109
phone: (415) 436-9333
fax: (415) 436-9993
e-mail: info@eff.org
website: www.eff.org

The Electronic Frontier Foundation was one of the first organizations established to support privacy rights in the online world. It provides information on laws relating to Internet privacy and works to ensure that governments and industries respect privacy rights.

Electronic Privacy Information Center

1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
phone: (202) 483-1140
fax: (202) 483-1248
website: <http://epic.org>

The Electronic Privacy Information Center focuses on safeguarding privacy in the digital age. It emphasizes traditional civil liberties. Its website includes articles and links to other useful sites.

Electronic Retailing Association

607 Fourteenth St. NW, Suite 530
Washington, DC 20005
phone: (703) 841-1751; toll-free: (800) 987-6462
fax: (425) 977-1036
e-mail: webadmin@retailing.org
website: www.retailing.org

The Electronic Retailing Association advocates for online retailers. The organization lobbies political leaders for laws that are favorable to forming connections between customers and businesses online.

International Association of Privacy Professionals

Pease International Tradeport
75 Rochester Ave., Suite 4
Portsmouth, NH 03801
phone: (603) 427-8200 • toll-free: (800) 266-6501
fax: (603) 427-9249
website: www.privacyassociation.org

This is an organization made up of people who work on privacy policies and similar matters for law firms, banks, and other corporations. The group's website offers details about changes in privacy laws as well as links to related articles.

Internet Alliance

1615 L St. NW, Suite 1100
Washington, DC 20036-5624
phone: (202) 861-2407
e-mail: tammy@internetalliance.org
website: www.internetalliance.org

The Internet Alliance is a nationwide group that advocates for the Internet industry. It lobbies for legislation that makes Internet commerce easier. It is intended primarily for businesses and government policy makers.

NetChoice

1401 K St. NW, Suite 502

Washington, DC 20005

phone: (202) 420-7498

fax: (202) 331-2139

e-mail: info@NetChoice.org

website: www.netchoice.org

Netchoice is a trade organization made up largely of online retailers and service companies. It attempts to make business on the Internet easier to conduct. In particular, it lobbies for the elimination of laws its members see as burdensome.

Privacy Rights Clearinghouse

3108 Fifth Ave., Suite A

San Diego, CA 92103

phone: (619) 298-3396

website: www.privacyrights.org

This organization is mainly concerned with the privacy rights of consumers. It offers information on issues such as identity theft, protecting the privacy of medical records, and ensuring that banks and other financial institutions do not divulge personal information to third parties without the consent of consumers.

Public Voice

e-mail: coney@epic.org

website: <http://thepublicvoice.org>

An arm of the Electronic Privacy Information Center, this organization focuses on the future of the Internet and the gathering of information worldwide. Its website includes a number of articles and alerts about online privacy.

Additional Reading

Books

Matthew Bailey, *Complete Guide to Internet Privacy, Anonymity, and Security*. Nerel, 2011.

Robert Curley, ed., *Issues in Cyberspace: From Privacy to Piracy*. New York: Britannica, 2012.

Stephen Currie, *Online Privacy*. San Diego: ReferencePoint, 2012.

Roman Espejo, *Social Networking*. Farmington Hills, MI: Greenhaven, 2012.

Nick Hunter, *Internet Safety*. Chicago: Heinemann, 2012.

Barbara M. Linde, *Safe Social Networking*. New York: Gareth Stevens, 2013.

Robert Plotkin, *Privacy, Security, and Cyberspace*. New York: Facts On File, 2012.

Daniel J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven, CT: Yale University Press, 2011.

Internet Sources

Consumer Reports staff, “Facebook and Your Privacy,” Yahoo! Finance, May 3, 2012. <http://finance.yahoo.com/news/facebook-and-your-privacy.html?page=1>.

COPPA—Children’s Online Privacy Protection Act, “Title XIII—Children’s Online Privacy Protection,” www.coppa.org/coppa.htm.

Jon Green, “We Don’t Need Facebook to Violate Our Privacy; We Do It to Ourselves,” *Americablog*, November 28, 2012. <http://americablog.com/2012/11/facebook-privacy.html>.

Glenn Greenwald, “XKeyscore: NSA Tool Collects ‘Nearly Everything a User Does on the Internet,’” *Guardian* (London), July 31, 2013. www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

Websites

American Civil Liberties Union (www.aclu.org). The ACLU is one of the organizations most strongly in favor of preserving privacy rights, including privacy on the Internet. The website includes information about the ACLU’s work and perspective.

State Laws Related to Internet Privacy, National Council of State Legislatures (www.ncsl.org/issues-research/telecom/state-laws-related-to-internet-privacy.aspx). This site provides a list of states that have passed laws regarding Internet privacy, as well as links to information on a number of other issues pertaining to online privacy.

Index

Note: Boldface page numbers indicate illustrations.

Abagnale, Frank, 31
activism and social media, 28
advertising, 27, 45, 51
American Civil Liberties Union (ACLU), 67, 75
anonymity of Internet, 40–43, 60
Apple
 cooperation of, with
 government information gathering, 49
 sale of information captured by, 45
 site tracking by, 43–44
Arizona, 76–77
Australia, 56

Bailey, Matthew, 63, 67–68
Bharara, Preet, 53
Bill of Rights, 11–13
blogging, 27
Boston Marathon, 28, **29**
Brown, Gary, 20
Buffett, Warren, 69
bullying, 36, 79
Bush, George W., 46
business
 as cybercrime targets
 annual cost of hackers to, 54

 example of, 52–54
 security measures and, 22, 62, 64, 65
 by state-sponsored Chinese, 56
government searches of
 records of, 46, 47–50
social media and
 advertisements on, 27
 employment and, 24, 33–34, 69
tracking customers' activities
 by
 Constitution and, 19
 customers' knowledge of, 24
 information harvested from, 39–43
 laws limiting information obtained by, 72–75
 opting out of, 43–44
 privacy policies and, 19, 44, 72–76, 79
voluntary guidelines for, 75–76

cell phones, 10, 20
Children Online Privacy Protection Act (COPPA, 1998), 72, 79
China, 56, 62
codes of conduct for business, 75–76

Cohen, Adam, 75
 Computer Fraud and Abuse Act (1986), 65
 computer viruses, 47, 63, 65
 Connecticut, 72
 Constitution, **13**
 cyberbullying and, 71
 overview of, 11–12
 private business and, 19
Consumer Reports (magazine), 44
 Cook, Johnny, 33
 cookies, use of, 51
 corporations. *See* business
 Coutts, Andrew, 45
 credit cards
 photographs of, 31, **32**
 theft of numbers on, 52–54, 57–58, 60–62
 cyberbullying
 described, 35–36
 laws concerning, 71–72, 79
 percent of students as victims of, 37, 79
 suicide and, 36, 71
 cybercrime
 keylogging, 63
 phishing, 63
 prosecution of, 52–53
 social media and, 28, 30, 31–32, **32**
 See also hacking
 databases
 created from online transactions, 40–43
 described, 20–21, 40
 government search of, 28, 48, 50
 security of, 22, 62, 64, 65
 debit cards. *See* credit cards
 Delaware, 73–74
 Department of Commerce, 76
 Department of Homeland Security, 65
 Drew, Lori, 71
 Egan, Roy, 33
 e-mail, privacy of, 14, 47, 77
 employment and social media, 24, 33–34, 69
 Europeans and Google Street View, 41
 Facebook
 government information gathering and, 28, 48, 49
 information tracked by, 44, **45**
 overview of, 25
 popularity of, 34, 37
 security settings' usage, 30, 33
 targeted advertising as business model of, 45
 Federal Trade Commission, 72
 Fertik, Michael, 70
 Fishman, Paul, 52–53
 Fourth Amendment, 12, 15, 18–19
 Freedom of Information Act, purpose of, 7
 free speech rights
 businesses and, 19
 cyberbullying laws and, 71
 described, 11–12
 limits to, 12
 gender and posting cell phone numbers online, 10

Google, 49
 Google Street View, 41
 government
 antiterrorism monitoring by
 described, 46–50
 public opinion about, 47,
 47, 50, 51
 citizens' online transactions
 with, 39
 Constitution and role of, 19
 fears about misuse of
 information collected by,
 45–46
 hacking of sites and
 databases of, 55, 65
 laws protecting privacy rights
 from, 76–78
 monitoring location of cell
 phone users by, 20
 public access to records of,
 6–9
 searches of records of
 business by, 46, 47–50
 technology and, 16–18
 warrants requirement
 accessing e-mail and, 77
 exceptions to, 20
 obtaining, 15
 purpose of, 46
 for use of imaging devices,
 18–19
 Green, Jon, 29–30
 Greenwald, Glenn, 48
Griswold v. Connecticut (1965),
 24
 gun permit holders and address
 controversy, 6–9
 hacking
 awareness of, 60, 61
 cost of, 54, 64, 65
 and credit card number theft,
 52–54, 57–58, 60–62
 database security and, 22, 62
 early, 55
 of government sites, 55, 65
 increase in, 62
 motivation for, 55, 57–58
 passwords and, 68
 prosecution of, 52–53, 65
 state-sponsored, 56
 techniques used in, 31–32,
 32, 63
 Hara, Billie, 35
 harassment online. *See*
 cyberbullying
 health information, 14, 30
 Health Insurance Portability
 and Accountability Act
 (1996), 14
 Heartland Payment Systems,
 53–54, 58
 Hibbert, Chris, 43
 Hindi, Ahen al-, 28
 Human Relations Media, 69
 identity theft, 31–32, 58–60, 65
 Illinois, 75
 Instagram, 34
 Internet
 advantages of, 21
 amount of personal
 information on, 22
 anonymity of, 40–43, 60
 entertainment uses of, 38
 global nature of, 23
 lasting nature of information
 on, 21
 See also Facebook; social
 media

- iPhones, site tracking by, 43–44
- jobs and social media, 24, 33–34, 69
- Journal News* (newspaper), 6–9
- Katz, Charles, 18
- Katz v. United States* (1967), 18, 20
- keylogging, 63
- Kurtz, Andrew, 33
- law enforcement
 - laws protecting privacy rights from, 13–14, 74, 76–78
 - monitoring location of cell phone users, 20
 - technology and, 16–18
 - warrants requirement
 - accessing e-mail and, 77
 - exceptions to, 20
 - obtaining, 15
 - purpose of, 46
 - for use of imaging devices, 18–19
 - See also* government
- laws
 - cyberbullying, 71–72
 - hacking, 65
 - obstacles to passage of, 75
 - protecting adults online, 72–73
 - protecting children online, 72
 - protecting privacy rights, 13–14, 74, 76–78
 - wiretapping, 24
- LinkedIn, 27, 61
- Los Alamos National Laboratory, hacking of, 55
- Maine, 76
- malware, 53, 65
- McNealy, Scott, 67
- Me and My 500 “Friends”*: *Staying Safe on Social Networks* (DVD), 69
- Meier, Megan, 71
- Microsoft, 49
- Minnesota, 73
- Missouri, 71
- Mitnick, Kevin, 55, 57
- Montana, 79
- Myspace, 25, 27, 37
- National Security Agency (NSA), 46–50, 47
- Nazi Germany, 46
- Nebraska, 73
- Nevada, 73
- New York, 6–9, 20
- online shopping, 39, 39–43, 51
- opting out of tracking, 43–44
- oversharing, 28–30, 36–37
- passwords, 42, 67–69, 79
- Patriot Act (2001), 46, 51
- “penumbra of the Bill of Rights,” 12–13, 24
- phishing, 63
- photographs online
 - of credit cards, 31, 32
 - identity theft and, 31–32
 - posted by friends, 69–71
 - used in harassment, 32–33, 79
- Pinterest, 27

Plotkin, Robert, 75
 Potter, Chris, 62
 Prince, Phoebe, 36
 PRISM program, 49
 privacy policies, 44, 79
 privacy rights
 absence of, in Constitution, 12
 businesses and, 19, 72–76
 do not exist on Internet, 67
 health information and, 14
 importance of, 66–67
 laws protecting, 13–14, 74, 76–78
 limits to, 14–15
 measures to help maintain, 42, 67–69, 79
 personal responsibility for, 78
 physical, described, 15–16
 restricting information
 obtained by government, 76–78
 social media can
 compromise, 29–30
 Supreme Court and
 “penumbra of the Bill of Rights” and, 12–13, 24
 “reasonable expectation of privacy” and, 18–19
 telephone conversations
 decision by, 18, 20
 public libraries, 76–77
 public opinion
 on government antiterrorism
 monitoring, 47, **47**, 50, 51
 on importance of privacy
 rights, 67
 on personal freedoms *vs.*
 terrorism, 10
 on targeted advertising, 51
 public places, 19–20
 public records, access to, 6–9

 Rambam, Steve, 67
 Raza, Ghyslaine, 35
 Reddit, 26
 reputation management
 companies, 70
 Robertson, Scott, 9
 Romania, hacking from, 62

 scamming, 63
 Scott, Ryan, 36
 7-Eleven, 53, 58
 Snapchat, 34
 Snowden, Edward, 49
 social media
 children on, 79
 criminal use of, 28, 30,
 31–32, **32**
 employment and, 24, 33–34,
 69
 government monitoring of,
 48
 information on
 about health, 30
 being careful about, 69
 life of, 21
 on oversharing of, 28–30
 resending of, 30–31,
 34–35
 instantaneous nature of,
 27–28
 overview of, 25, 27
 public shaming on, 26
 security settings and, 34–35
 state laws concerning, 74–75
 use by teenagers, 34, 37, 79
 See also Facebook

Social Security Administration records, 22, 24
 Social Security numbers, 43, 51, 65
 Sony, 60–61
 Soviet Union, 46
 spying and state-sponsored hacking, 56
 Stalin, Josef, 46
 “Star Wars Kid,” 35
 Supreme Court
 “penumbra of the Bill of Rights” and, 12–13, 24
 “reasonable expectation of privacy” and, 18–19
 telephone conversations decision, 18, 20
 targeted advertising, 45, 51
 technology
 Supreme Court decisions and, 18–20
 telegraph, **16**, 16–17
 telephone, 17–18, 20, 47–48
 teenagers. *See* youth
 terrorism, public opinion
 about ceding personal freedoms to fight, 10
 thermal imaging and privacy, 18–19
 Twitter, 27, 37
 University of Connecticut, 61–62
 USA Patriot Act (2001), 46, 51
 viruses, computer, 47, 63, 65
War Games (movie), 55
Wikipedia (online encyclopedia), 38
 wiretapping, 18, 24, 46
 Wisnefski, Kenneth, 28
 Wyndham Hotels, 62
 XKeyscore program, 48, 50
 youth
 cyberbullying and described, 35–36
 laws concerning, 71–72, 79
 and percent of students as victims, 37, 79
 suicide and, 36, 71
 early hacking by, 55
 Facebook use by, 34, 37
 learning about misusing social media, 69
 and online protection of children, 72
 posting cell phone numbers online, 10
 Zappos, 61
 Zuckerberg, Mark, 25, 67

Picture Credits

Cover: iStockphoto.com

Andre Jenny Stock Connection Worldwide/Newscom: 61

AP Images: 8, 29, 39, 45, 47

© Furgolle/BSIP/Corbis: 22

© Heritage Images/Corbis: 17

© Brendan McDermid/Reuters/Corbis: 54

Thinkstock Images: 13, 32, 59, 68, 73, 77

About the Author

Stephen Currie is the author of several dozen books for young adults and other readers. He has also written magazine articles, educational materials, and other works, and he has taught levels ranging from kindergarten to college. He lives with his family in New York State.