CQ Researcher

Published by CQ Press, a Division of SAGE

www.cqresearcher.com

Online Privacy

Do Americans need better protection?

The Internet has become not only a primary means of communication but a place where millions of Americans store important personal data, from credit-card numbers and bank account information to family photos and histories of their online purchases. But that data does not have the same legal protection as data that Americans store in their homes. What's more, powerful new technologies are creating unexpected challenges to privacy online. Advertisers, for example, can now track the Web sites you visit, and actions you take on those sites, to analyze how to more effectively sell products to you. And they may sell the information they collect to others. Privacy advocates, and some lawmakers in Congress, say the growing threats to online privacy point to the need for stronger laws to protect users' data. But Republicans in Congress warn that overregulation may cripple the economic foundation of the Internet.

Consumers' visits to online shopping sites — as well as other sites — now can be tracked with new electronic tools by advertisers, Internet service providers and backers.

INSIDE THIS REPORT

CQ Researcher • Nov. 6, 2009 • www.cqresearcher.com
Volume 19, Number 39 • Pages 933-956

CQ PRESS

RECIPIENT OF SOCIETY OF PROFESSIONAL JOURNALISTS AWARD FOR EXCELLENCE ◆ AMERICAN BAR ASSOCIATION SILVER GAVEL AWARD

ONLINE PRIVACY

Cover: CQ Press/Screenshot

CQ Researcher

Nov. 6, 2009
Volume 19, Number 39

MANAGING EDITOR: Thomas J. Colin
tcolin@cqpress.com

ASSISTANT MANAGING EDITOR: Kathy Koch
kkoch@cqpress.com

ASSOCIATE EDITOR: Kenneth Jost

STAFF WRITERS: Thomas J. Billitteri, Marcia Clemmitt, Peter Katel

CONTRIBUTING WRITERS: Rachel Cox, Sarah Glazer, Alan Greenblatt, Reed Karaim Barbara Mantel, Patrick Marshall, Tom Price, Jennifer Weeks

DESIGN/PRODUCTION EDITOR: Olu B. Davis

ASSISTANT EDITOR: Darrell Dela Rosa

EDITORIAL INTERN: Emily DeRuy

FACT-CHECKING: Eugene J. Gabler, Michelle Harris

CQ PRESS

A Division of SAGE

PRESIDENT AND PUBLISHER: John A. Jenkins

CQ Researcher (ISSN 1056-2036) is printed on acid-free paper. Published weekly, except; (Jan. wk. 1) (May wk. 4) (July wks. 1, 2) (Aug. wks. 3, 4) (Nov. wk. 4) and (Dec. wk. 4), by CQ Press, a division of SAGE Publications. Annual full-service subscriptions start at $803. For pricing, call 1-800-834-9020, ext. 1906. To purchase a *CQ Researcher* report in print or electronic format (PDF), visit www. cqpress.com or call 866-427-7737. Single reports start at $15. Bulk purchase discounts and electronic-rights licensing are also available. Periodicals postage paid at Washington, D.C., and additional mailing offices. POSTMASTER: Send address changes to *CQ Researcher*, 2300 N St., N.W., Suite 800, Washington, DC 20037.

Online Privacy

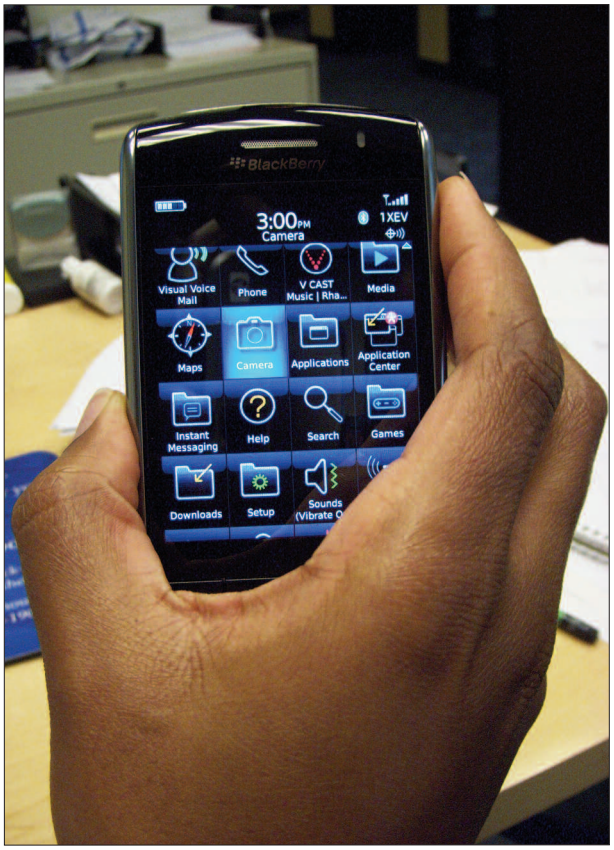
By Patrick Marshall

The Issues

Could this happen to you? You return home from vacation to find your apartment has been burglarized. In your snail mail is a notice from your health insurer canceling your policy. And when you check your e-mail your minister is asking why you recently purchased a book about devil worship.

Privacy experts say such things happen countless times a day because of new electronic tools that allow Internet service providers, advertisers, hackers and others to track consumers' Web searches, site visits, e-mails and social networking sites.

For instance, burglars reading your Facebook page could easily find out when you are going on vacation. Even if you don't include your home address, a criminal may easily be able to find the information on your profile page. Your health insurer may have canceled your insurance after receiving information from a marketing firm whose online survey you just completed in hopes of winning a new iPod. And when you bought the devil worship book out of curiosity online, the information about the purchase was automatically posted to your Facebook friends, including your minister.



CQ Press/Olu Davis

Cellphones are increasingly being used to provide location information, such as where to find the nearest pizza or the cheapest gasoline. Law enforcement agencies are also turning to service providers to obtain location information on subjects of investigation, raising concern among privacy advocates that Americans' privacy rights could be violated.

"With social networking, people are leaving trails of digital DNA sprinkled about everywhere in the world," says Tim Sparapani, director of public policy at Facebook.

But the danger isn't just limited to social networking sites like Facebook, say privacy advocates; for example:

• A Dartmouth University professor said he retrieved tens of thousands of medical files — including names, addresses and Social Security numbers — from a peer-to-peer network, or system of linked computers. [1]

• The wife of a senior British intelligence official inadvertently revealed sensitive information in postings to her Facebook site. [2]

• An investment firm employee inadvertently exposed information about clients, including Social Security numbers, when he logged into a peer-to-peer network to share music and movie files. [3]

• A graphic designer in Seattle used Craigslist to pose as a woman seeking sexual encounters and then posted all 178 responses he got to an open Web site, including photographs and personal contact details. [4]

But most online privacy intrusions never receive public attention, despite the growing number of incursions that have come to light in recent years.

"With the advent of personal Web sites, blogs, social networks and Twitter, people are sharing information about themselves that would certainly make their grandparents blush," Richard Bennett, publisher of *BroadbandPolitics.com*, told lawmakers on Capitol Hill in April. "Stories abound about young people who've posted drunken party pictures of themselves while they were in college finding the embarrassment often costly when they apply for jobs and have to explain their antics to Google-savvy recruiters. The Internet is a harsh mistress, and much of what happens there stays there, seemingly forever." [5]

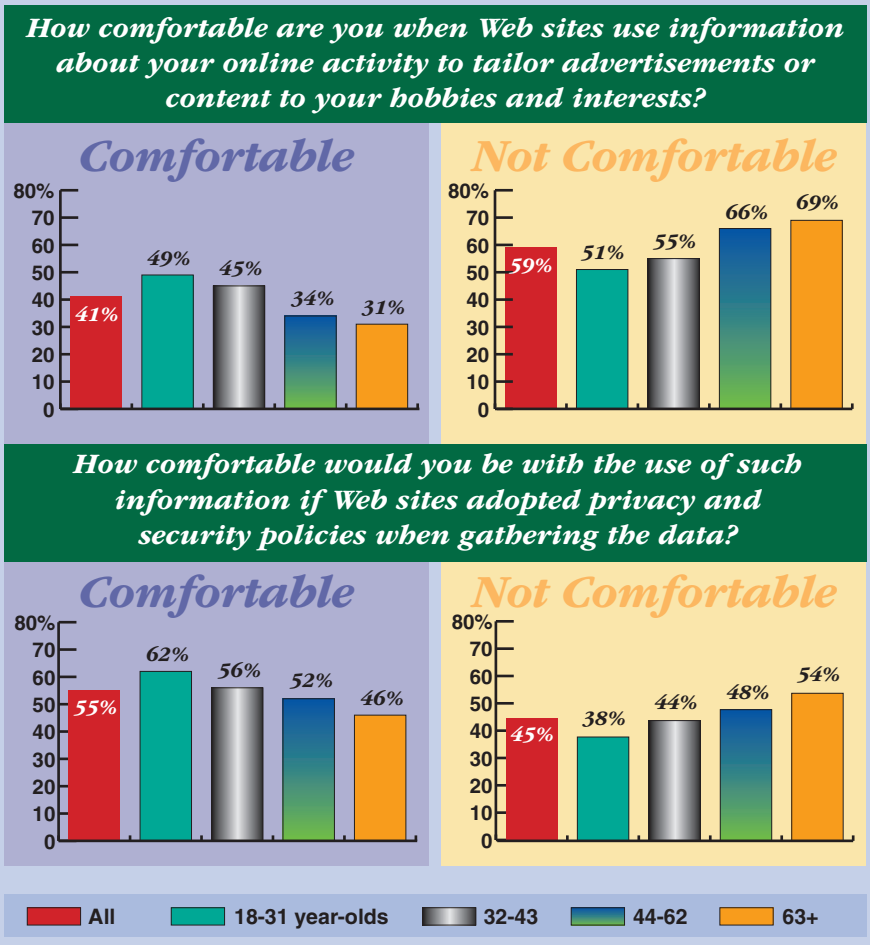
Avoiding social networking sites is not, however, a guarantee of privacy. Internet service providers (ISPs) and search engine providers can learn a good deal about customers by tracking the searches they make.

Search engines, indeed, offer a deep mine of data. In fact, according to one count, Americans performed more than 13 billion searches in September alone. [6] The search engines typically record not only the terms searched for but also the date, time and location of the computer performing the search. While search engine companies generally "anonymize" records of searches, that is no guarantee of complete anonymity.

In addition, advertisers and their agents are able to track the Web activities of

Internet Users Welcome Privacy Polices

Most Internet users — especialy older people — are uncomfortable when Web sites use data about their online activities, but when privacy and security measures are put in place, a majority of users feel comfortable.



Source: The Harris Poll, April 2008

users by the use of "cookies" — small text files that are deposited on users' computers when they visit a site.

Finally, service providers — as well as hackers, government agencies and anyone else who can tap into the flow of Internet traffic — can also employ "packet analysis" to examine the content of users' unencrypted communications across the Internet.

It's no surprise that these technologies are extremely popular with Internet advertisers. In fact, the highest-profile current threat to online privacy, according to most privacy advocates, is a new practice called "behavioral targeting" of advertising. By tracking users' actions on specific Web sites and their movements across many sites, advertisers develop user profiles and then target advertising to individual users based on their profiles.

A user might, for example, visit an airline site looking for flights to New York City, then might search for opera CDs. An advertising service following that user's movements might then deliver ads to the user's browser offering tickets to the Metropolitan Opera.

While some users might find such targeted ads helpful, others may feel that having their Web activities tracked and recorded is intrusive. Even those who don't mind the targeted advertising may not like the idea that their Internet activities could potentially be reported to other parties. For example, would users about to apply for health insurance want the insurer to know that they had recently been searching for "symptoms of colon cancer"?

Indeed, when Charter Communications, the nation's fourth-largest cable company, announced in the spring of 2008 that it was preparing to deliver just such advertising services in conjunction with a company called NebuAd, complaints from consumers and privacy advocates prompted congressional hearings. Apparently as a result of fallout from the hearings, NebuAd lost so many clients that it went out of business.

While Charter dropped its plan, others are picking up the idea. A recent study by Datran Media, an advertising consulting group, found that 65 percent of marketers currently use or plan to use behavioral targeting. [7]

"The private sector as a whole has tremendous technical means and tremendous economic incentives to collect as much granular data as they can about as many customers as possible," says Jay Stanley, director of public education at the American Civil Liberties Union. "That kind of information about people is money. And in a capitalist system people don't leave money lying around unpicked."

Of course, advertisers aren't the only ones interested in users' online activities. Users' privacy is under even more significant threat from the federal government, according to Stanley. "The National Security Agency is monitoring our telecommunications," he says, including Internet communications.

In addition, he notes, the government has easy access to a broad swath of the data being collected by service providers. "While the private sector is collecting all this information because of its own incentives," says Stanley, "the legal protections against the government swooping in and getting it are precisely what have been loosened over the past decade." Stanley cites in particular provisions of the USA Patriot Act regarding warrantless searches of electronic data. [8]

Recent polls show that advocacy groups aren't the only ones concerned about Internet privacy. According to the *Consumer Reports* National Research Center, 72 percent of American adults polled in July 2008 were concerned that their online behaviors are being tracked and profiled by companies. [9] In addition, 93 percent of respondents believe Internet companies should ask for permission before using personal information.

"I do think users are starting to feel a little bit out of control," says Ari Schwartz, vice president of the nonprofit Center for Democracy and Technology.

There have been several unsuccessful attempts in recent years to legislate stronger protections for online users' data. In the current Congress, the highest-profile effort is being led by Rep. Rick Boucher, D-Va., who has promised to introduce legislation aimed at regulating data collection by advertisers and service providers.

As privacy advocates, advertisers and consumers debate the privacy issue, here are some of the questions being asked:

Should advertisers' collection of data on Web users be regulated?

Advertisers — working with ISPs, search engine providers and individual Web sites — are turning to ever more powerful tools to gather information about users so that they can more accurately target their ads. There

Ten Ways to Protect Your Facebook Privacy

Facebook users cannot control all the photos and videos of themselves that show up on other people's Facebook pages, but they can adjust the privacy and invisibility settings on their own profiles. If you are a Facebook user, here are ways to protect your privacy:

1. *Use Friend Lists* You can create groups of friends by type and send messages to each group. Friends can be in more than one group, and different groups can have different privacy settings applied to them.

2. *Remove Self from Facebook Search Results* By default, Facebook makes your presence visible to people in your network. You can change your privacy settings, however, so that only certain groups, such as your social friends, can see your information.

3. *Remove Self from Google* Facebook displays your profile picture, a list of your friends, a link to add you as a friend, a link to send you a message and a list of your fan pages in search engines. By changing your privacy settings, you can control the visibility of your public search listing.

4. *Avoid Photo, Video Tag Mistakes* You can be fired at work for incriminating photos and videos, or even suffer damage to relationships. You can, however, keep tagged photos private or make them visible only to some friends.

5. *Protect Your Photo Albums* People often turn off tagged photo visibility to certain friend lists, yet keep their photo albums public. If you want your photos to be invisible, you must adjust your privacy settings for each album.

6. *Prevent Stories From Appearing in Friends' News Feeds* You can hide your relationship status completely, or you can avoid making things uncomfortable if your status does change by preventing friend notification. You can prevent friend notification for other stories, as well.

7. *Protect Against Unpublished Application Stories* When you add an application, a news feed item is often immediately published in your profile. You should check your profile to ensure that no embarrassing notification has been posted, or avoid using applications entirely.

8. *Make Contact Information Private* Many people make contact information public, such as phone numbers and e-mail addresses. If you want that information kept private, or you start receiving messages from strangers, you can create custom privacy settings for each contact listed. Again, you can allow certain friend lists to see certain contact information.

9. *Avoid Embarrassing Wall Posts* You may use Facebook for business, but not all of your friends will. You can customize the visibility of your wall postings and control which friends post to prevent work colleagues from seeing embarrassing recaps of the weekend.

10. *Keep Friendships Private* You may like to show off that you have lots of friends, but your friends may not want to live public lives. It is often a good idea to turn off your friends' visibility to others so that others do not visit your profile and selectively pick off your friends, such as those relevant to them for marketing purposes or other reasons.

Source: Nick O'Neill, "10 Privacy Settings Every Facebook User Should Know," All Facebook*, Feb. 2, 2009, www.allfacebook.com/2009/02/facebook-privacy/*

are, however, very few checks on what advertisers and service providers can do with the data.

"Users have little idea how much information is gathered, who has access to it or how it is used," Marc Rotenberg, executive director of the Electronic Privacy Information Center (EPIC) and a professor at Georgetown University Law Center, told Congress last spring. [10] "This last point is critical because in the absence of legal rules, companies that are gathering this data will be free to use it for whatever purpose they wish — the data for a targeted ad today could become a detailed personal profile sold to a prospective employer or a government agency tomorrow."

In fact, in most cases the only constraints on service providers in their collection and use of personal data are their own privacy policy statements. According to Peder Magee, senior staff attorney in the Federal Trade Commission's Division of Privacy and Identity Protection, if a company's practices violate its published promises, "that would be a deceptive claim and something we could take some action against."

Privacy advocates warn, however, that some service providers don't offer promises about privacy at all. "As long as you don't actually promise anybody any privacy — and companies have gotten very good at writing privacy policies that contain all kinds of warm, ringing tones about how they care for your privacy without actually making any legal commitments — then they don't have to deliver any," says Stanley at the American Civil Liberties Union.

As Stanley notes, even sites and service providers that do offer privacy statements generally do so in the form of rarely read, long and difficult-to-understand documents buried under an obscure link on a Web site. As a result, many if not most users are unaware of the extent of data being gathered about them and the uses to which it may be put.

With or without their knowledge, "people are giving information to a Web site in order for that site to provide them with a service," says Stanley. "They don't expect that Web site will then turn around and share the information with six other sites, combine the information to create a profile and give it to an advertiser who will decide whether you're rich or poor and give you different opportunities as a result."

Most users are also unaware that their Internet searches are recorded and can be used for profiling. "Internet search records are very, very intrusive records," says Stanley. "The things that you do searches for indicate your hopes and fears, what you're thinking about, what you may be reading, diseases that you have and diseases you fear you might have, things you believe about other people."

Advertisers justify collection of user data on two grounds. First, they argue that advertising is critical to keeping the Web vibrant. "The great majority of . . . Web sites and services are currently provided to consumers free of charge," Charles Curran, executive director of the Network Advertising Initiative, an industry group, told a congressional hearing last June. [11] "Instead of requiring visitors to register and pay a subscription fee, the operators of Web content and services subsidize their offerings with various types of advertising. These advertising revenues provide the creators of free Web content and services — site publishers, bloggers and software developers — with the income they need to pay their staffs and build and expand their online offerings."

Second, advertisers argue the collection of user data helps advertisers better serve consumers. "Targeted advertising is extraordinarily important for everybody," says Dan Jaffe, vice president of government relations for the Association of National Advertisers. That, he says, is because the more information advertisers have about users the fewer irrelevant ads will be delivered to those users.

Conversely, Jaffe says, restrictions on behavioral targeting won't cut down on advertising. "A lot of people seem to think that if they can stop behavioral advertising that they will somehow stop advertising," he says. "Quite the contrary. Instead, you'll see an explosion of untargeted ads. You'll essentially increase the amount of spam because spam is, in effect, untargeted advertising."

Rather than legislated restrictions on advertising practices, the advertising industry argues that self-regulation — including full disclosure through clear privacy statements and procedures for users to opt out of selected data-collection programs — should be sufficient to protect users' privacy interests.

Berin Szoka, director of the Center for Internet Freedom, a project of the Progress & Freedom Foundation, a "market-oriented" think tank in Washington, agrees. "I think industry can do this on its own," says Szoka. "We should want companies to really make disclosures robust so that people really understand what they're doing." Then, he says, leave it up to the Federal Trade Commission to deal with companies that violate their privacy agreements. "They should be going out and finding the truly bad actors in industry and bringing enforcement actions against them," Szoka urges. "If they need more resources, we can talk about that."

Szoka adds that user education is another important part of the solution. "What we should be doing here is trying to educate users about what is going on online and empowering them to make decisions for themselves," he says. "If you really are very concerned about your privacy online, you have a very simple tool. You can go into your browser and use the basic cookie controls to opt out of browsing

altogether, or site by site. You can create your own white lists or black lists. I would like to see those tools become much more powerful."

Privacy advocates, however, are very skeptical of self-regulation. "While we remain hopeful that advertising models based on non-personally identifiable information can be made, there are still too many instances where companies, particularly where there is no regulation, fail to fulfill their responsibilities," Rotenberg of the Electronic Privacy Information Center (EPIC) told lawmakers last spring.

"Second, even if these privacy techniques are shown to be reliable, it will still be necessary to enact legislation to place the burden on the advertising company to prevent the reconstruction of user identity," he added. "Without this statutory obligation, there would be no practical consequence if a company inadvertently disclosed personal information or simply changed its business model to true user-based profiling."

Are social networking sites doing enough to protect users' privacy?

Privacy advocates maintain that social networking sites present special challenges for privacy protection because the sites by design encourage users to offer and share personal information.

According to Facebook's Sparapani, the information-sharing nature of social networking sites is actually a plus for privacy awareness, in the sense that when people post data they know it is being shared. "Rather than having information randomly collected about you," says Sparapani, "you know what is being collected about you because we're telling you forthrightly. You can then go claim that data and put your own stamp on it."

Critics note, however, that users may not be aware that the data they provide is available not only to their designated friends but also to advertisers, albeit with personal identifiers removed. And many are not aware

A Glossary of Common Internet Terms

Behavioral Targeting — *A type of targeted advertising in which advertisers glean information from user data to tailor ads to user interests, limiting irrelevant ads.*

Cloud — *A metaphor for the Internet, based on how the Internet is depicted in computer network diagrams. Cloud computing services provide business applications online that are accessed from a browser, while the software and data are stored on servers.*

Cookie — *A message given to a browser by a server, which is then sent back to the server each time the browser requests a page. Identifies users and prepares customized Web pages for them.*

Cookie controls — *Some kinds of cookies facilitate tracking of Internet users or store identifying information. Cookie controls let users decide which cookies can be stored on their computers or transmitted to Web sites.*

Deep-packet inspection — *The examination of contents of Internet transmissions using "packet analysis" software. In addition to content transmitted by users, such as passwords or e-mails, each packet in a transmission contains the address of its origin and destination and information that connects it to the related packets being sent.*

GPS — *The Global Positioning System is a network of satellites and software that provides positioning, navigation and timing services to worldwide users. Many cellphones now include GPS receivers and software that allow the delivery of location-based services to users.*

Location-based services — *software programs that employ GPS to deliver a variety of information related to users' current location, such as routing or information about nearby points of interest, such as stores or restaurants.*

Privacy mode — *Browsers typically retain visited Web sites, downloaded files, terms searched, data — including passwords — typed into online forms, and cached versions of files locally on users' computers. Privacy mode reduces local storage of this information, providing increased privacy on shared computers.*

Web browser — *A software application used to locate and display Web pages, such as Internet Explorer and Mozilla Firefox.*

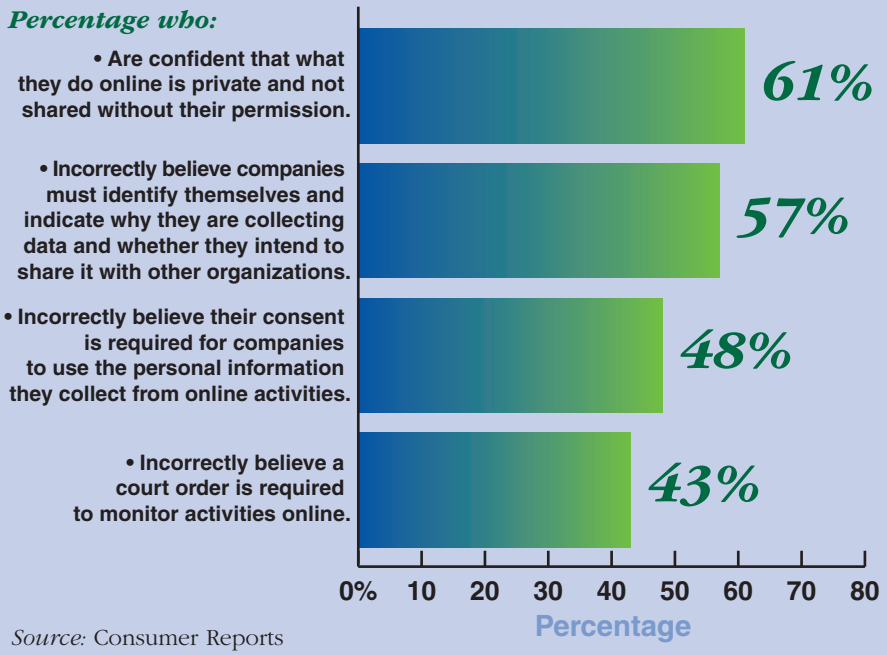
Web server — *A computer program, such as Apache, that delivers Web pages to browsers as well as other data to Web-based applications.*

Source: "Browser Privacy Features: A Work in Progress," Center for Democracy and Technology, August 2009, www.cdt.org/privacy/20090804_browser_rpt_update.pdf; "Definitions," Webopedia, *Oct. 29, 2009, www.webopedia.com/.*

Many Internet Users Ill-Informed About Privacy

More than 60 percent of Internet users are confident that their online activities are private and cannot be shared without their permission. A similar percentage, though, incorrectly thinks Internet companies are mandated to disclose their intentions for collecting data. And about half incorrectly believe that consent is required for companies to use personal information collected from users.

What Internet Users Think About Priviacy



Source: Consumer Reports

that when they access any of the applications made available on Facebook — from quizzes and games to movie guides — by default the application developers have access not only to the users' data but also to that of friends of the users.

"Consciously or unconsciously you're in a marketing environment," says Lillie Coney, EPIC's associate director. "If you have a pet, you might be more inclined to give to an animal rescue group. Is that fair to use a consumer? Did you know that what you are seeing is being influenced by the communications you share with others who are your intimate friends in a social networking context? Should that be used in a way to sell you something?"

Coney also worries that the collection of data on social networking sites could lead to "differential marketing," in which not only the products but also the prices offered to users vary depending upon their characteristics. "Are you being presented items at prices that are based on your ability to pay rather than the quality of the item?" she wonders. "They can change the price depending on your profile."

In response to concerns voiced by users and privacy advocates, many social networks — including MySpace and Facebook — have recently introduced extensive enhancements to user privacy controls protecting what information on a user's site is made available to different parties. Users can, for example, prevent applications from having access to personal data.

"Some people want to share everything about themselves at all times with everybody," says Sparapani. "Other people don't want to share much with anybody at all. And everyone else falls in between. What Facebook has done is not just provide privacy controls, it is actually for the first time giving people at every level of the spectrum abilities to do exactly what they want or don't want with their data."

What's more, Sparapani emphasizes that when Facebook does share users' data with third parties, it is always stripped of personally identifiable data.

"We sell ad space, and we agree to serve ads to demographics that you tell us to target," says Sparapani. "But we never turn around and give you data other than to say, yes, your ads were served to these following groups of people with these demographic characteristics. It's a really important distinction."

Facebook also has taken steps to protect users from application developers who might abuse user data. Users can now block applications entirely or block them from accessing personal data.

Also, says Sparapani, "We do spot-checks of applications." Facebook staff review applications to see what data they are gathering and whether it is relevant to their apparent purpose. "We also have built the platform such that no application can access the most sensitive information that you have on your profile, such as contact information."

Coney acknowledges that Facebook has made significant strides in improving privacy controls and statements. "It is very important that companies are making an effort," she says. "It is important that they recognize that privacy is a major issue with their consumers."

At the same time, Coney says the efforts aren't enough. "A lot of these sites give an impression that they are private," she says. "But the privacy notices

are so complicated. I know they're written with concern about liability exposure, but they have to be simpler."

Sparapani contends that the best protection is an educated user base. And he praises the capabilities of the majority of Facebook users. "Our users are really quite savvy as a group," he says. "Our users are the best police force out there. They know when an application doesn't do what it says it does, or when it does more than it should, and they feel free to report us, and then we initiate a review of that specific application."

Many users, however, are not so savvy, says Coney, noting, "That's why we have regulatory agencies that stand up for the consumers."

While agreeing that educating users is a crucial step, Coney argues that broader protections for personal information are needed. "We also need to see a uniform foundation for privacy protection established," she says. "This requires the regulatory agencies such as the Federal Trade Commission to establish a regulatory framework that companies have to operate in, and it requires Congress to establish laws that are not technology centric but that are based on collection and use of personally identifiable information."

Do federal privacy policies regarding the Internet need to be updated?

Calls for changes in federal policies regarding privacy on the Internet come primarily on two fronts: use of cookies on federal Web sites and revision of the Electronic Communications Privacy Act of 1986 (ECPA), the primary federal legislation regulating non-commercial aspects of Internet activity.

Issued in 2000, current federal cookie policy prohibits federal agencies from using cookies and other tracking technologies on federal Web sites. "There is an exception to that, which is used quite rarely: If the department or agency head makes a finding that there's a compelling need to use a cookie, the agency or department can do so," says a senior Office of Management and Budget (OMB) official, who agreed to be interviewed without being named. For example, the official said, Web sites operated by the National Aeronautics and Space Administration and the National Institutes of Health have received such exemptions.

Last June, however, the OMB began seeking comments to the following proposed changes in this policy: Federal Web sites would be allowed to employ Web tracking technologies as long as they post clear and conspicuous notice on the Web site, provide a clear and understandable means for users to opt-out of such tracking and do not limit users' access to information if they opt-out of the tracking. [12]

The suggestion has alarmed privacy advocates. "This is a sea change in government privacy policy," Michael Macleod-Ball, acting director of the Washington legislative office of the American Civil Liberties Union (ACLU), said in a press release in August. "Without explaining this reversal of policy, the OMB is seeking to allow the mass collection of personal information of every user of a federal government Web site. Until the OMB answers the multitude of questions surrounding this policy shift, we will continue to raise our strenuous objections."

According to the OMB official, the policy change is not a done deal. "There are no actual proposed changes in the sense that anything is hardwired to be changed," he says. While he acknowledges that cookies carry potential privacy concerns, he says "making certain that people's privacy is protected in an extremely robust way is going to be a paramount concern of this administration, should any changes be proposed."

At the same time, he said, "it may be the case that there are ways in which judicious use of cookies on government Web sites can enable the Web sites to be more interactive, more robust, richer in terms of content and features and capabilities, so that they can really enable government to work better for people. That is the animating goal here."

While most privacy advocates oppose changes to existing cookie policies on federal Web sites, most advocacy groups are calling for major changes to ECPA on the grounds that the 1986 legislation is seriously out of date and no longer adequately protects sensitive data.

"This very important law, which I think in many ways does effectively protect people's privacy online, has understandably become outdated as the pace of technological change has increased," says Kevin Bankston, a senior attorney at the Electronic Frontier Foundation. "There are at this point fundamental questions about what ECPA protects that are unanswered and maybe are unanswerable without additional congressional guidance."

According to Bankston, nothing more pointedly demonstrates how out of date ECPA is than its provisions regarding e-mail. "E-mail is a technology that actually existed in 1986, and ECPA was drafted with that in mind," he says. "And yet there still critical questions about how ECPA applies to e-mail."

Under ECPA, for example, an electronic communication that has been in electronic storage with an electronic storage provider for 180 days or fewer requires a warrant if the government wants to access it. "The reason 180 days is required is because of differences in the past technology," says Bankston. "Back in 1986, when you dialed into your e-mail service and you downloaded your e-mail, it was erased off the server. So if you had left your e-mail there for six months, the fair assumption was that you had abandoned it and therefore it was not deserving of special protection."

What's more, says Bankston, a number of emerging technologies aren't specifically treated under ECPA. The

issue of how ECPA applies to the government getting data from Internet search logs is, he says, "completely unsettled."

While Bankston and other privacy advocates call for reforms in ECPA, no party is actively opposing such reform. Many privacy advocates, however, believe that the Department of Justice would prefer to see the current law remain as it is. "I think it is fair to say that they may be resistant," says Jim Dempsey, vice president for public policy at the Center for Democracy and Technology. "To some extent, the Justice Department is doing a good job of manipulating the ambiguities and the loopholes in the statute now."

While he did not directly respond to Dempsey's charge of manipulating ambiguities and loopholes in ECPA, a Department of Justice official says, "We've been looking for places where there are gaps and trying to resolve issues. We've also been working within the structure created by Congress, which tried to be technology neutral to some extent in passing the statute. Where there are interpretive gaps, we are presenting that to the courts. And there is opportunity, of course, to have the courts interpret the statute.

"I wouldn't say ECPA is out of date," added the official, who asked that his name not be used. "I would say there are concepts in it where Congress might have had a technology in mind when it was legislating and that technology is no longer in place. The courts have then tried to adapt to newer technologies that replaced it."

Nor has Congress actively taken up the issue of ECPA reform in recent years. According to Dempsey, "Up until now the issues have been discussed and debated only among the true ECPA nerds. It is a relatively small community of people who know about the statute, who understand the statute and who see how it works, so up until now the issue has not received a lot of public prominence." ■

Consumer Electronics Association (Boucher)
Getty Images/Johnathan Ernst (Stearns)

Rep. Rick Boucher, D-Va., (left), chairman of the House Subcommittee on Communications, Technology and the Internet, says he will introduce legislation this fall to protect online privacy. Rep. Cliff Stearns, R-Fla., favors consumer education efforts and industry self-regulation and warns against overregulation.

BACKGROUND

Tracking Technologies

From 1967, when the Internet was born, until the mid-1990s, privacy was a non-issue. There was no advertising, no security measures apart from log ins, no spam and, until 1989, no graphic interfaces — no icons, images, windows, etc.

It was not until 1994 that the first tracking tool — the "cookie" — was introduced by Netscape Communications to check on whether visitors to the Netscape Web site had been there before. Early advertisers also found uses for cookies. When users downloaded pages from a Web site that included an advertisement or other content from the advertiser's server, a "third-party cookie" could also be included. That enabled advertisers not only to determine when their ads were viewed but also to detect what other sites the user visited where that cookie was also present.

Initially, cookies attracted little public notice. Users were not informed when cookies were deposited on their computers, and Web browsers did not have tools for blocking cookies. It wasn't until the *Financial Times* of London published an article about cookies in February 1996 that the general public knew about cookies. By that time, a working group of the Internet Engineering Task Force, an international standards group, identified cookies — and especially third-party cookies — as a potential threat to user privacy.

While the task force recommended that third-party cookies not be allowed, or at least be blocked by browsers by default, both Netscape and Microsoft Corp. — makers of the two dominant browsers — declined to follow the recommendation.

But, while cookies may present risks for user privacy, they also offer convenience and a richer Web experience. For example, cookies can be used to allow automated logins to Web sites or

Continued on p. 944

Chronology

1980s-1990s

Internet service providers (ISPs) and advertisers develop tools for tracking user visits and online behaviors.

1986
Electronic Communications and Privacy Act (ECPA) protects transmissions of electronic data by computers.

1994
First Internet tracking tool — the "cookie" — is introduced by Netscape Communications to check users' visits to its Web site.

1995
DoubleClick Web advertising company begins using cookies to track Internet users' Web visits.

1996
Internet Engineering Task Force identifies cookies as a potential threat to privacy. The next year the group calls for third-party cookies — those that feed data to a party other than the visited Web site — to be disabled in Web browsers. Microsoft and Netscape — the two major browser makers — reject the recommendation.

1998
Children's Online Privacy Protection Act of 1998 restricts the collection for commercial purposes of personal information about children under age 13.

1999
Network Advertising Initiative, launched by 12 advertising companies, begins developing standards for Internet advertising. . . . Federal Trade Commission holds its first workshop on behavioral targeting in Internet advertising.

2000s

Federal government begins to look more closely at legislation and regulation to protect Web users as Internet service providers, advertisers and federal agencies get more sophisticated in user tracking.

2000
Clinton administration sets strict rules on the use of cookies on federal Web sites. . . . FBI introduces Carnivore program for monitoring Internet users' activities.

2001
USA Patriot Act amends ECPA to allow the FBI to access data by simply issuing "National Security Letters" to ISPs, rather than obtaining a warrant.

2005
A disgruntled employee reveals on her blog that Kaiser Permanente had inadvertently posted private patient information on its Web site. The healthcare provider is ultimately fined $200,000 by the state of California.

2006
Department of Justice asks federal judge to force Google to turn over user-search queries as part of an investigation of violations of online pornography laws; Google successfully resists the subpoena. . . . America Online makes the records of 20 million subscriber searches available to Internet researchers; some users are identified, underscoring the potential for privacy incursions.

2007
Facebook's Beacon advertising campaign uses information gathered from users' activities on other Web sites that are partnering with Facebook. After public criticism, Facebook changes the program to track users' activities only if they specifically opt-in to the program. . . . Sen. Patrick Leahy, D-Vt., introduces Personal Data Privacy and Security Act of 2007, aimed at enhancing criminal penalties and increasing reporting requirements. The bill does not come to a vote in the full Senate. . . . Ask.com announces that it will allow users to control whether their search terms are saved by the search service, a move applauded by privacy advocates. . . . *The Washington Post* reveals that federal officials are routinely asking courts to order cellphone companies to furnish real-time tracking data so they can pinpoint the whereabouts of drug traffickers and other suspects.

2008
Charter Communications, an ISP, and NebuAd, an advertising company, announce plans to analyze subscribers' Internet traffic and then tailor ads to users whose profiles indicate a match of interests; congressional lawmakers hold hearings and pressure the companies to abandon the project. . . . A federal judge in Pittsburgh declines prosecutors' attempts to obtain people's cellphone tracking information without a warrant.

2009
House Subcommittee on Communications, Technology and the Internet holds hearing on behavioral targeting by Internet advertisers. . . . Office of Management and Budget proposes loosening federal restrictions on use of cookies on federal Web sites. . . . National Archives and Records Administration concedes it sent a defective hard drive back to a vendor before erasing the health records of as many as 70 million veterans. . . . Canada's privacy commission reports that Facebook violates Canadian privacy laws in four areas and gives the site 30 days to change its policies.

Is Data Storage 'in the Cloud' Safe?

Privacy advocates warn there is no legal protection.

Back in the early days of the Internet, users stored their personal information on floppy discs and the hard drives of their computers.

That's all changed now. Increasing numbers of users are storing data on the Internet — or "in the cloud" — and using cloud applications, such as Google Apps, or cloud data storage like Microsoft LiveMesh. The convenience is obvious: Once data is stored online, it can be accessed from any Internet-connected computer.

But privacy advocates warn that the legislation protecting the privacy of users' data hasn't changed to keep up. As a recent story on National Public Radio noted, while the checkbook sitting in your desk at home is protected by the Fourth Amendment from being accessed by government agents without a warrant, that protection may not apply to data you keep in an online checking account. [1]

And since the data is stored remotely it may be difficult for users to even know how vulnerable it is. Is the third-party server holding the data reliable? Is the data encrypted, or is it susceptible to theft by hackers? Are there assurances the storage company will not share the data with others? What if the company shuts down the service, or the government asks the company for access to a customer's stored data or a party to a lawsuit demands the data?

Privacy advocates warn, for example, that some cloud service providers claim to "support" various security technologies — such as data encryption — when those technologies may not be enabled by default (automatically) and may require the user to request them.

Indeed, in June 38 researchers and academics in computer science, information security and privacy law signed a letter to Google asking the company to follow through on protecting the data of users of its cloud applications by turning on the supported HTTPS Web-encryption technology. [2] Google engineer Alma Whitten replied, "We're currently looking into whether it would make sense to turn on HTTPS as the default for all G-mail users," as well as for users of other Google cloud applications. [3]

While no major problems have occurred thus far with cloud storage, privacy advocates say clear, legal protections for stored data don't exist. In fact, according to a recent report by the World Privacy Foundation, data stored in the cloud may have more than one legal location, with differing legal consequences depending upon the location.

"A cloud provider may, without notice to a user, move the user's information from jurisdiction to jurisdiction, from provider to provider or from machine to machine," the report notes. "The legal location of information placed in a cloud could be one or more places of business of the cloud provider, the location of the computer on which the information is stored, the location of a communication that transmits the information from user to provider and from provider to user, a location where the user has communicated or could communicate with the provider, and possibly other locations." [4]

The foundation cautions users that the application of current privacy law to the data stored in the cloud is "unpredictable," in that the courts, without clear direction from Congress, are applying the laws inconsistently. What's more, it warns, "The government is not the only entity that might seek to obtain a user's record from a cloud provider. A private litigant or other party might seek records from a cloud provider rather than directly from a user because the cloud provider would not have the same motivation as the user to resist a subpoena or other demand."

— Patrick Marshall

[1] Martin Kaste, "Online Data Present A Privacy Minefield," "All Things Considered," National Public Radio, Nov. 4, 2009, www.npr.org/templates/story/story.php?storyId=114163862.

[2] http://files.cloudprivacy.net/google-letter-final.pdf.

[3] http://googleonlinesecurity.blogspot.com/2009/06/https-security-for-web-applications.html.

[4] Robert Gelman, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing," World Privacy Forum, Feb. 23, 2009, p. 7.

Continued from p. 942

to deliver content that is customized according to user preferences. And Web site managers can use the information in cookies to improve the design and navigation of sites by seeing how users traverse pages.

While there is no federal law governing the use of cookies on non-governmental Web sites, the Clinton administration in 2000 set strict rules on cookie use at federal Web sites following disclosures that the White House Office of National Drug Control Policy had used cookies to track users visiting its site.

Search engine logs represent another rich source of user data. The search engine technologies that concern privacy advocates, however, were developed relatively late in the game to enhance security and the user experience.

The first software tool for searching the Internet was a program called Archie. Created in 1990, it simply sought out and downloaded directory listings of files on public FTP (file transfer protocol) sites. Archie did not index or display the contents of the files.

The Web's first actual search engine — Aliweb — debuted in November 1993. Unlike today's search engines, which send out "robots" to visit Web sites and generate an index of contents, Aliweb relied on Web site administrators to submit links to index files.

The first program developed to "crawl" the Web to find sites and index them for searching was JumpStation, which appeared in December 1993, but it indexed only titles and headings rather than the entire contents of pages.

Beginning in 1994, several search engines appeared that performed full-text indexing of Web sites. It wasn't until 2000, however, that a clear winner — Google — emerged in the race to become the dominant search engine. Google introduced page ranking, which allowed users to more quickly and reliably retrieve Web sites of interest, using search terms. By 2008, Google accounted for more than 82 percent of search engine traffic worldwide.

The key concern privacy advocates have about search engines is the electronic logs that they keep of users' searches. According to Google, the logs are primarily generated to help in improving the service. By examining search activity coming from a specific Internet Protocol (IP) address — and each computer on the Internet is assigned a unique IP address — the company can detect problems developing on the network.

"The ability on Google's side to look at what is happening from a particular IP address over time is the kind of thing that we often look at to prevent abuse or to do certain kinds of machine learning on," says Alma Whitten, a Google software engineer. More specifically, says Whitten, Google engineers will monitor the logs to look for patterns that may tip off the presence of "denial of service" attacks. And engineers use the logs in an effort to improve the algorithms that make searches possible.

Advertisers Self-regulate

As early as 1995, the pioneering Web advertising firm DoubleClick began using cookies to track users on the Web.

CQ Press/Screenshot (both)

Government and Private Industry Sites

Federal agencies are prohibited by federal policies from using "cookies" and other tracking technologies on their Web sites. However, some sites, including those operated by the National Institutes of Health (top), have received exemptions. Proposed changes in federal policies regarding the Web have alarmed privacy advocates, who say the changes would "allow the mass collection of personal information of every user of a federal government Web site." In response to concerns voiced by users and privacy advocate, many social networks — including Facebook (bottom) — have recently introduced extensive enhancements to user privacy controls protecting what information on a user's site is made available to different parties.

At the same time, some in the advertising industry also realized that while tracking technology offered opportunities for marketing, it also represented a challenge to consumer confidence.

"Back in the early 1990s, the few people trying to use [the Internet for marketing] were being flamed [criticized] because a lot of people on the Internet claimed that it should be a marketing-free zone," recalls Jaffe, at the Association of National Advertisers. "We said back then that if this was going to be an effective medium, adequate concern about consumer privacy issues had to be one of the pillars it was built on."

In fact, most efforts to ensure privacy protections with respect to marketing on the Internet have been accomplished through self-regulation with the assistance and oversight of the Federal Trade Commission (FTC). The one legislative exception to this is the Children's Online Privacy Protection Act of 1998, which placed restrictions and requirements on the collection for commercial purposes of personal information of children under the age of 13. [13]

The Network Advertising Initiative (NAI), a nonprofit industry group formed by 12 companies, was created in 1999 to work with the FTC to develop a set of principles to govern Internet advertising efforts. The principles basically required NAI member companies to post a notice on all Web sites served by their networks informing users the advertiser may place a third-party cookie on their computers. In addition, members were required to offer an opt-out tool for users who didn't want targeted ads from NAI members, and to refrain from merging personally identifiable information with Web browsing data without users' opt-in.

The FTC convened a town hall forum with industry representatives in 2007 to discuss the need for further regulation of online adverting activities. After the forum, the NAI issued revised guidelines in December 2008 that expanded members' commitment to provide security for data and also required:

- Consumer opt-in for "sensitive" information used with behavioral targeting, such as health conditions or treatments, and location information;
- Parental consent to use non-personally identifiable data to target behavioral advertising to children under age 13, and
- An annual in-house compliance review.

Similar standards were adopted by another industry group, the Interactive Advertising Bureau, in 2008.

While efforts at self-regulation may have provided some assurances to the public, they have not slowed the use of tracking cookies or newer tracking technologies, such as deep-packet inspection, by advertising firms and service providers. (*See glossary, p. 939.*)

The limitations on self-regulation became clear to the public and to Congress in 2008, when Charter Communications, an Internet service provider, and NebuAd, an advertising company, announced plans to perform deep-packet inspection on subscribers' Internet traffic. By examining users' activities on the Web, the companies planned to tailor ads and target them to users whose profiles indicated a match of interests.

Congressional hearings resulted in the plans being dropped. But while some legislators argued that the proposed practice violated existing wiretap and privacy laws, no legislation resulted that might clarify the legality of deep-packet inspection.

Some analysts on Capitol Hill tie the prospect for privacy legislation to growing public awareness and concern. "It's clear that the technology exists to monitor where consumers go and what they do on the Internet. It's also clear that a lot of companies are looking to monetize it," Jessica Rosenworcel, senior communications counsel for the Senate Commerce panel, said after the hearings last spring. "What is less clear is what consumers are aware of and what they're comfortable with." [14]

Federal Tracking

Congress has generally taken a hands-off approach to Internet privacy issues, except for the Electronic Communications Privacy Act of 1986. ECPA basically extended federal restrictions on wiretaps of telephone calls to protect transmissions of electronic data by computers. Title II of the act, the Stored Communications Act, protects communication held in storage, specifically e-mails, though with less stringent protections than are accorded under Title I, which protects transmissions. Under Title II, if an unopened e-mail has been in storage for 180 days or less, the government must obtain a search warrant to access it.

ECPA's protections were weakened by the USA Patriot Act of 2001, which allowed the FBI to access data by simply issuing so-called National Security Letters to ISPs, which allow FBI investigators to obtain information without a warrant.

"So once the private companies gather and store the information, it is there to be plucked by the government with very little judicial oversight," says the ACLU's Stanley. "Basically, the Patriot Act took judges out of the equation."

While Congress has shown reluctance since 1986 to weigh in on online privacy issues — even to bring the provisions of ECPA up to date with respect to changes in Internet technologies — the executive branch has made repeated efforts to expand its capabilities to monitor Internet activity.

The FBI introduced its Carnivore program in 2000 to conduct Internet surveillance — purportedly under the guidance of ECPA. The software, which was apparently a tool for deep-packet analysis, attracted such negative coverage in the media that the name was changed to DCS1000. The bureau apparently abandoned Carnivore in 2005

in favor of other commercially available monitoring tools.

In 2002, the U.S. Defense Advanced Research Projects Agency proposed developing an Internet surveillance system — "Total Information Awareness" — that would monitor content across the Internet. The project apparently was dropped after the U.S. Senate voted for restrictions on its development in 2003.

That same year, the Bush administration announced plans to build an Internet monitoring center to detect and respond to attacks on key systems. The Global Early Warning Information System was to be developed under the National Communications System, a Defense Department agency.

The Department of Justice has repeatedly taken Google to court in an effort to gain access to search records. In 2005, for example, the DoJ filed a motion in federal court to force Google to comply with a subpoena for the text of search "strings" entered into the search engine over a one-week period. The court granted part of the request, but denied the government access to users' specific search strings. [15]

The next year the Department of Justice again asked a federal judge to force Google to turn over user search queries as part of an investigation of violations of online pornography laws. Google successfully fought the subpoena. [16]

In April 2008 the FBI called for legislation that would allow federal law enforcement agencies to monitor Internet traffic for "illegal activity." [17] ■

CURRENT SITUATION

Action in Congress

Internet privacy for consumers is attracting some attention in Congress.

In April the House Energy and Commerce Subcommittee on Communications, Technology and the Internet, chaired by Virginia Rep. Boucher, held hearings on consumer privacy. And in June the House Energy and Commerce Subcommittee on Commerce, Trade and Consumer Protection, chaired by Rep. Bobby Rush, D-Ill., held hearings specifically on behavioral targeting of online advertising.

Boucher and Rush have made clear that the two subcommittees are working closely together in conducting hearings. "There are currently no federal laws specifically governing behavioral advertising nor do we have a comprehensive general privacy law," Rush noted in opening the June hearings. "As members of Congress, we have anticipated for some time that this hearing would be highly informative and very valuable in helping us answer the question that everyone seems to ask: Is federal privacy legislation necessary, or should companies be trusted to discipline and regulate themselves?"

Boucher has been more assertive in his view that legislation is necessary. "I think that as far as they go the voluntary codes that have been adopted within the industry are constructive," Boucher told *CQ Researcher*. "They represent a step forward. The problem is that not every Web site will be a part of that voluntary commitment." As a result, Boucher has promised to introduce legislation during the current Congress, promising that it will be bipartisan.

While Democrats on both subcommittees seem generally more inclined toward regulating online advertisers, Republicans seem to prefer self-regulation. Nevertheless, comments by committee members during the hearings suggest there is room for bipartisanship. "It is still a little bit of a Wild West out there [on the Internet], and I think it is time that Congress begins to look at and try to bring some law and order to that particular Wild West area," Rep. Joe Barton, R-Texas, said. [18]

Rep. Cliff Stearns, R-Fla., said he favored consumer education efforts and warned the hearing against overregulation. "Consumers' online activities provide advertisers with valuable information upon which to market their products and their services," Stearns said. "Collecting this type of information for targeted advertising is very important because it simply allows many of these products and services to remain free to consumers. Without this information, Web sites would either have to cut back on their free information and services or would have to start charging a fee. Neither result is good for the consumers." [19]

Stearns added that "Overreaching privacy regulation could have a significant negative economic impact at a time when many businesses in our economy are struggling, so let us be very careful on these issues before we leap to legislative regulatory proposals."

While the privacy of consumer data is receiving increasing attention, government access to users' online data is drawing relatively little attention, although many privacy advocates say government access is potentially the greater threat.

Federal monitoring programs tend to have a lower profile because they generally take place behind the scenes, say privacy advocates. Internet monitoring by the super-secret National Security Agency and other intelligence organizations, of course, is classified information and rarely subjected to public scrutiny. And even cases involving the Department of Justice are rarely in the spotlight.

"At some level the Justice Department retains control over the cases that emerge into the public light," says the Center for Democracy and Technology's Dempsey. "A lot of recipients of government orders are generally prohibited from disclosing their existence. And they don't necessarily want to disclose the order because they don't want to scare their customers.

Is Your Smartphone Keeping Tabs on You?

Advertisers and police tune in, but civil libertarians worry.

Global positioning system (GPS) chips in cellphones and mobile navigation devices have turned location-based services into a booming industry. Already some cellphone applications and auto GPS devices tell you where to find pizza close by, or the cheapest gasoline.

Indeed, according to *The Wall Street Journal*, location-based services will be a $13-billion-a-year business by 2013, compared to $515 million last year. [1]

But it's not just advertisers who are interested in accessing cellphone and vehicle location information. Law enforcement agencies are increasingly turning to service providers to obtain location information on subjects of investigation.

The laws applying to such actions, however, are not clear. "Federal officials are routinely asking courts to order cellphone companies to furnish real-time tracking data so they can pinpoint the whereabouts of drug traffickers, fugitives and other criminal suspects, according to judges and industry lawyers," noted *Washington Post* reporter Ellen Nakashima. "In some cases, judges have granted the requests without requiring the government to demonstrate that there is probable cause to believe that a crime is taking place or that the inquiry will yield evidence of a crime." [2]

"The question of what legal process the government needs to follow to track your cell phone is hotly disputed in front of magistrate judges across the country," says Kevin Bankston, an attorney with the Electronic Frontier Foundation.

Bankston says his group only became aware of the issue in 2005, mainly because such government actions generally are kept secret. "Typically, we don't know what is going on at that level," he explains. "It all occurs under seal. Unless something comes out at a criminal trial, we don't know what they're doing."

Under the circumstances, says Bankston, "The only solution is Congress — it could step in and provide clear rules for cellphone tracking."

Some privacy advocates also point to the potential for abuse of location information from "other" parties, such as stalkers and domestic abusers.

In recent congressional testimony, Leslie Harris, president of the Center for Democracy and Technology, called for three measures, the first two of which would require congressional action:

- The disclosure of precise location information in a commercial context must only be made with specific, informed, opt-in consent in which a user has the ability to selectively disclose locations only to trusted parties. As Congress contemplates enacting baseline consumer privacy legislation, such a requirement could easily be part of a broader framework governing sensitive consumer data.
- The standards for government and law enforcement access to location information must be amended to make clear that a probable-cause warrant is required for the government to obtain location information.
- Location-based services and applications should follow technical standards that give users clear control over the use of their location information and that require the transmittal of privacy rules with the location information itself. [3]

— Patrick Marshall

[1] Amol Sharma and Jessica E. Vascellaro, "Companies Eye Location-Services Market," *The Wall Street Journal*, Nov. 21, 2008, http://online.wsj.com/article/SB122722971742046469.html.

[2] Ellen Nakashima, "Cellphone Tracking Powers on Request, Secret Warrants Granted Without Probable Cause," *The Washington Post*, Nov. 23, 2007, www.washingtonpost.com/wp-dyn/content/article/2007/11/22/AR2007112201444.html.

[3] Statement before House Energy and Commerce Subcommittee on Communications, Technology and the Internet, April 23, 2009.

"The companies grapple with these issues quietly behind the scenes, in negotiations with the Justice Department," Dempsey continues. What's more, privacy advocates note, the Justice Department has near complete control over the cases it chooses to litigate. "The Justice Department will drop charges or decide not to use the evidence against anybody in a case that might be going against them," says Dempsey. "So the Justice Department gets to go public with the issues only in the context of drug trafficking, child abuse and terrorism — those cases the deptartment prefers to talk about."

Accordingly, some privacy advocates believe that one of the most important reforms needed in the Electronic Communications Privacy Act is requirements for reporting. "Right now the government can bend the rules and make really outrageous arguments," says Bankston of the Electronic Frontier Foundation. "Because the proceedings are sealed, and there's no adversary there to point out when the government is overreaching, they can in fact get powers that were not given to them by Congress for years at a stretch before they are found out. This problem could be addressed if Congress were to require reporting."

Privacy advocates note that privacy threats occur in part because legislative and regulatory policies generally seem to trail behind the capabilities of emerging technologies.

"Our courts have not kept up with technology and have not kept up with

Continued on p. 950

At Issue:

Should Congress regulate online behavioral advertising?

JEFF CHESTER
EXECUTIVE DIRECTOR,
CENTER FOR DIGITAL DEMOCRACY

FROM TESTIMONY BEFORE HOUSE SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY AND THE INTERNET, JUNE 18, 2009

Some in the online ad industry appear to suggest that any legislative attempt to place consumers in charge of their online data would undermine the economic role of the Internet media. But I believe that by legislatively creating a system where consumers can be assured that their data are protected and transactions are structured to further empower them, trust and confidence in our online marketplace will grow and thrive. I firmly believe that we can protect privacy and also see the online marketplace and medium prosper.

Behavioral targeting and related technologies may provide "marketing nirvana," as one company explained, but it leaves consumers unaware and vulnerable to an array of marketing communications that are increasingly tied to our financial and health activities.

[Advertisers'] privacy policies are an inadequate mechanism that fail to protect the public. As documented in a recent University of California-Berkeley School of Information study on online privacy, privacy policies are difficult to read; the amount of time required to read them is too great; they lead consumers to falsely believe their privacy is protected; there [aren't] meaningful differences between policies, leaving consumers with no alternatives; and consumers aren't really aware of the "potential dangers.

The FTC [Federal Trade Commission] has been largely incapable of ensuring American privacy is protected online. Staff has been reined in from more aggressively pursuing the issue, primarily to ensure that industry self-regulation remains as the agency's principal approach.

The FTC needs to have additional resources, especially so it can better protect consumers from digital marketing transactions involving their financial and health data. Congress should press the FTC to be more proactive in this arena.

The failure to adequately regulate the financial sector greatly contributed to the worst economic crisis since the Great Depression. Regulation isn't a dirty word. It's essential so consumers and businesses can conduct their transactions with assurance that the system is as honest and accountable as possible.

The uncertainty over the loss of privacy and other consumer harms will continue to undermine confidence in the online advertising business. That's why the online ad industry will actually greatly benefit from privacy regulation. Given a new regulatory regime protecting privacy, industry leaders and entrepreneurs will develop new forms of marketing services where data collection and profiling are done in an aboveboard, consumer-friendly fashion.

BERIN SZOKA (LEFT)
DIRECTOR, CENTER FOR INTERNET FREEDOM
ADAM THIERER
DIRECTOR, CENTER FOR DIGITAL MEDIA FREEDOM
PROGRESS & FREEDOM FOUNDATION

FROM "ONLINE ADVERTISING AND USER PRIVACY: PRINCIPLES TO GUIDE THE DEBATE," SEPTEMBER 2008

To the extent that effective, self-help privacy tools exist, they provide a means of solving policy problems that is not only "less restrictive" than government regulation but generally more effective and customizable as well. Why settle for one-size-fits-all solutions of incomplete effectiveness when users can quite easily and effectively manage their own privacy?

Fortunately, a wide variety of self-help tools and "technologies of evasion" are readily available to all users and can easily thwart traditional cookie-based tracking, as well as more sophisticated tracking technologies, such as packet inspection.

The "free" Internet economy is based on a simple value exchange: Users get access to an ever-expanding collection of content and services at no cost from Web sites that are able to generate revenue from "eyeballs" on their pages by selling space on their sites to advertisers, usually through ad networks. The smarter that advertising, the more free content and services it can support.

As users face an increasingly clear choice between (1) getting content and services for free supported by behavioral advertising and (2) paying to receive those same services and content without tracking or even without ads altogether, policy makers will finally see whether users are really as bothered by profiling as the advocates of [online behavioral advertising] regulation insist. Given the ongoing and widespread replacement of fee- or subscription-supported Web business models with ad-supported models, it seems likely that the vast majority of consumers will continue to choose ad-supported models, including profiling.

Indeed, if smarter online advertising will not fund the Internet's future, what will? As both the desire for "free" services and content and the need for bandwidth expand, [online behavioral advertising] has the potential to offer important new revenue sources that can help support the entire ecosystem of online content creation and service innovation, while also providing a new source of funding for Internet infrastructure and making ads less annoying and more informative.

But looming legislative and regulatory action could stop all of that by replacing the current regime — in which the FTC merely enforces industry self-regulatory policies — with one in which the government preemptively dictates how data may be collected and used.

Continued from p. 948

the needs of privacy," says the ACLU's Stanley. "When the Fourth Amendment was written, most of people's lives took place in the home. Your medical life, your correspondence, your financial records were in the home. And the founding fathers recognized the need for privacy and put in strong protections for privacy in the home. But much of our lives are now stored on the servers of international corporations. And yet we have not extended privacy to cover that."

One solution to that problem suggested by some privacy advocates is adoption of an information-centric approach to privacy, rather than the current technology-centric approach.

"We're interested in getting a comprehensive privacy law," says Schwartz of the Center for Democracy and Technology. "Right now, we have laws protecting medical privacy and video rental records. But we don't have the general overarching privacy law that some other countries do."

Advertisers Press Ahead

While Internet service providers have apparently acceded to pressure from Congress to refrain from monitoring users' Internet activity, search engine companies and advertisers are moving ahead. Most notably, Google last March launched its own behavioral targeting program, "AdSense." The program tracks Web visits and search terms in order to build a profile of users' interests. Google is then able to display targeted ads when a user visits a participating Web site.

To avoid the complaints that ultimately sank NebuAd, Google allows users to opt out of the program and to view and edit the categories they are assigned to by Google based on their Web site visits.

"Because we're very aware that people might have privacy concerns about this, we've put a great deal of effort into being very transparent about how this will work," says Google software engineer Whitten.

"On any of those ads where we're doing this there is a link across the bottom, and if the user clicks on that they get taken to a page where Google explains how this works and gives them the opportunity to view the interest categories that Google has associated with their cookie and offers to let them opt out of the whole thing," explains Whitten. "We've made sure that all of the categories involved are very innocuous." According to Whitten, the categories include such interests as cooking, travel and sports. More personal and intrusive topics, such as cancer and political affiliations, are not included.

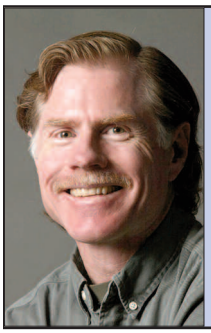
Schwartz at the Center for Democracy and Technology praises Google's decision. "We're targeted in so many ways and in so many categories" by advertisers, he says. "There's discussion about what kind of information is sensitive. You hear less concern about that when Google makes the categories they are targeting available. It doesn't solve every problem to make them available and let you change them, but it helps."

Microsoft is reportedly also working hard on developing behavioral targeting tools, though the company declined comment.

And some social networking sites have moved into providing behavioral targeting services for advertisers. In 2007 Facebook introduced its Beacon advertising campaign, which uses information gathered from a user's activities on other Web sites that are partnering with Facebook. If, for example, consumers purchase books at Amazon.com, an item about those purchases might appear on their page. Facebook did offer an opt-out to users, but the service nevertheless attracted so much criticism that the company scaled back Beacon in several important ways. First, and most significantly, Beacon now only works with users who choose to opt in to the program.

At the same time that major advertising companies and service providers are refining and developing behavioral targeting programs, they are working closely with each other and with the Federal Trade Commission to develop self-regulation standards for the rapidly emerging capabilities. And not coincidentally, both the FTC and a coalition of advertisers this year released reports on self-regulation of behavioral-targeted advertising programs.

On Feb. 12, the FTC issued its report, citing as one of the primary reasons the fact that "staff recognized that existing self-regulatory efforts had not provided comprehensive and accessible protections to consumers. Accordingly, in issuing the proposed principles, staff intended to guide industry in developing more meaningful and effective self-regulatory models than had been developed to date." [20]



About the Author

Patrick Marshall is a freelance writer in Seattle, Wash., and contributing writer for *CQ Researcher* who writes about public policy and technology issues. He is a computer columnist for *The Seattle Times* and holds a BA in anthropology from the University of California at Santa Cruz and a master's in international studies from the Fletcher School of Law & Diplomacy at Tufts University.

The four broad principles are:

• **Transparency and control:** Companies should provide "meaningful disclosures" about the practice and choice about whether to allow it.

• **Security and data retention:** Companies should provide reasonable data security measures and should retain data "only as long as necessary for legitimate business or law enforcement needs."

• **Material changes:** Before a company uses data in a manner that is "materially different" from promises made when the company collected the data, it should obtain "affirmative express consent" from the consumer.

• **Sensitive data:** Before using data about children, health or finances, companies should obtain affirmative express consent.

The report noted that the FTC had received many objections from industry representatives about proposals requiring companies to receive affirmative, express consent before using data in a materially different manner and before collecting sensitive data.

Nevertheless, the commission vote to approve the report was unanimous. However, in a concurring statement included in the report, Commissioner Jon Leibowitz warned advertisers, "Industry needs to do a better job of meaningful, rigorous self-regulation, or it will certainly invite legislation by Congress and a more regulatory approach by our commission. Put simply, this could be the last, clear chance to show that self-regulation can — and will — effectively protect consumers' privacy in a dynamic, online marketplace."

Several months after the FTC issued its report the coalition of advertisers released its own, identically titled report. [21] Moreover, the industry principles are nearly identical with the FTC's, except regarding consent required for collecting sensitive data or making material changes in the use of data. While the FTC calls for requirements that users must actively "opt-in," the industry group would see an individual's refraining from opting out of the system as sufficient. [22]

For now, the FTC is taking a wait-and-see approach to attempts at self-regulation. "We felt when we released the principles that companies need to do a much better job," says senior staff attorney Magee. "Since our principles came out, we have seen some positive steps by business. But we probably haven't had enough time to see the full impact of them and how some of these self-regulatory programs are going to be operationalized and what it is going to mean to consumers.

"It's a good start. But how long we support that approach and how long Congress holds off on legislating remains to be seen." ■

OUTLOOK

'A Number of Issues'

Chairman Boucher of the House Subcommittee on Communications, Technology and the Internet intends to introduce legislation this fall to regulate behavioral targeting in online advertising.

"There are a number of issues that we will seek to address," says Boucher. "Fundamental to all the protections we're proposing will be a requirement that any Web site that collects information from Internet users have a clear statement on the Web site of what information is collected and provide to the Internet user the opportunity to opt out of having any information collected."

Boucher adds that there would be further requirements for more sensitive data, such as financial and medical data as well as any information about children.

But Boucher also intends to offer advertisers a "safe harbor." If advertisers follow a specified set of "best practices," their data collection would be subject only to opt-outs by consumers. Opt-ins, which advertisers argue are much more difficult to obtain from consumers, would not be required.

"We're looking at a growing list of possible practices that would fit within that category and trying to make some determination at this point as to where the line is drawn," says Boucher. "That is a work in progress. We've not drafted a bill yet. We're still at the information-collection stage on this question . . . and we may ultimately decide to leave that determination to the Federal Trade Commission."

For its part, the advertising industry continues to warn against relying on legislation for regulating online advertisers. "A lot of people ask, 'Why not have legislation to solve the problem?' " says Jaffe at the Association of National Advertisers. "Because locking in policy in an area that is changing as rapidly as this is risky. Where technology is changing rapidly, almost inevitably legislation stands in the way of innovation and misses the target and is overly rigid."

Some members of Boucher's subcommittee during the April hearing also expressed hesitation about regulating the online advertising industry. "As we move forward towards privacy legislation, we must empower consumers to make their own privacy-related decisions," said Florida Rep. Stearns, the subcommittee's ranking Republican. "Only the consumer knows how he or she feels about the information that is being collected, the parties doing the collecting and the actual purpose for which the information will ultimately be used. Congress cannot and should not make that decision for them." [23]

Privacy advocates, for their part, would like to see something even broader than what Boucher has in mind. While some interest groups are calling for a comprehensive privacy law that focuses on people's data rather than the technology used to collect it, others argue the

law should give citizens an advocate when it comes to privacy.

"This is an area where you need privacy guardians who have some power and who are dedicated to privacy issues to monitor and regulate," says the ACLU's Stanley. "The European Union and most every industrialized country have privacy commissioners who have the power to do that."

As for providing protections from government monitoring of online data, privacy advocates concede that progress will be slow. "On the Electronic Communications Privacy Act front, I do believe that the civil liberties organizations and industry are coming close to reaching a consensus position to put before Congress," says Bankston of the Electronic Frontier Foundation.

But that's only the beginning of the process, says Dempsey at the Center for Democracy and Technology. "It will be a long effort, and actually achieving legislation will require "a long and cautious process," he says. "We have to educate the members of Congress. We have to, to a certain extent, educate the public." ■

FOR MORE INFORMATION

American Civil Liberties Union, 125 Broad St., 18th Floor, New York, NY 10004; www.aclu.org. Provides education and legal support for civil liberties issues.

Association of National Advertisers, 708 Third Ave., 33rd Floor, New York, NY 10017; (202) 296-1883; www.ana.net. Provides information, advocacy and lobbying efforts for the advertising industry.

Center for Democracy and Technology, 1634 Eye St., N.W. #1100, Washington, DC 20006; (202) 637-9800; www.cdt.org. Advocates and informs on privacy, copyright and openness to keep the Internet "open, innovative and free."

Center for Digital Democracy, www.democraticmedia.org. "Works to promote an electronic media system that fosters democratic expression and human rights."

Electronic Frontier Foundation, 454 Shotwell St., San Francisco, CA 94110-1914; (415) 436-9333; www.eff.org. EFF defines itself as "the leading civil liberties group defending your rights in the digital world."

Electronic Privacy Information Center, 1718 Connecticut Ave., N.W., Washington, DC 20009; (202) 483-1140; www.epic.org. Provides information as well as lobbying and advocacy efforts on a wide range of privacy issues.

Network Advertising Initiative, 62 Portland Road, Suite 44, Kennebunk, ME 04043; (207) 467-3500; www.networkadvertising.org. An industry organization formed to develop standards for online advertising.

Privacy Rights Clearinghouse, 3100-5th Ave., Suite B, San Diego, CA 92103; (619) 298-3396; www.privacyrights.org. An advocacy group and clearinghouse that assembles a great deal of information from varied sources on privacy issues.

Progress and Freedom Foundation, 1444 I St., N.W., Suite 500, Washington, DC 20005; (202) 289-8928; www.pff.org. Describes itself as "a market-oriented think tank that studies the digital revolution and its implications for public policy."

Notes

[1] See www.tuck.dartmouth.edu/faculty/publications/forum/johnson.html.

[2] Sarah Lyall, "On Facebook, a Spy Revealed (Pale Legs, Too)," *The New York Times*, July 6, 2009, p. A1.

[3] Brian Krebs, "Justice Breyer Is Among Victims in Data Breach Caused by File Sharing," *The Washington Post*, July 9, 2008, p. A1.

[4] Matthias Schwartz, "Malwebolence," *The New York Times*, Aug. 3, 2008, p. MM24.

[5] Testimony before House Energy and Commerce Subcommittee on Communications, Technology and the Internet, April 23, 2009.

[6] www.comscore.com/Press_Events/Press_releases/2009/10/comScore_Releases_September_2009_U.S._Search_Engine_Rankings.

[7] See www.reuters.com/article/pressRelease/idUS148003+27-Jan-2009+MW20090127.

[8] For background, see the following *CQ Researcher* reports: Kenneth Jost, "Civil Liberties Debate," Oct. 24, 2003, pp. 893-916; Kenneth Jost, "Government Secrecy," Dec. 2, 2005, pp. 1005-1028; Marcia Clemmitt, "Privacy in Peril," Nov. 17, 2006, pp. 961-984.

[9] See www.consumersunion.org/pub/core_telecom_and_utilities/006189.html.

[10] Statement of Marc Rotenberg, executive director, EPIC, and adjunct professor, Georgetown University Law Center, before House Energy and Commerce Subcommittee on Communications, Technology and the Internet, April 24, 2009.

[11] Statement of Charles Curran, executive director, Network Advertising Initiative, before House Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection and Subcommittee on Communications, Technology and the Internet, June 18, 2009.

[12] http://blog.ostp.gov/category/cookie-policy/.

[13] For background, see Marcia Clemmitt, "Cyber Socializing," *CQ Researcher*, July 28, 2006, pp. 625-648.

[14] Adrianne Kroepsch, "Deeper Ad Probes Sound Web Alarm," *CQ Weekly*, May 11, 2009, p. 1076.

[15] See http://epic.org/privacy/gmail/doj_court_order.pdf.

[16] See www.google.com/press/images/ruling_20060317.pdf.

[17] See http://news.cnet.com/8301-10784_3-9926899-7.html.

[18] Preliminary transcript of the hearing available at: http://energycommerce.house.gov/Press_111/20090618/transcript_20090618_ct.pdf.

[19] *Ibid.*

[20] "Self-regulatory Principles for Online Behavioral Advertising," Federal Trade Commission, February 2009, p. 11.

[21] "Self-regulatory Principles for Online Behavioral Advertising," American Association of Advertising Agencies, Association of National Advertisers, Council of Better Business Bureaus, Direct Marketing Association, Interactive Advertising Bureau, July 2, 2009.

[22] *Ibid.*, p. 10.

[23] "House Energy and Commerce Subcommittee on Communications, Technology and the Internet Holds Hearing on Communications Networks and Consumer Privacy: Recent Developments," CQ Congressional Transcripts, Congressional Hearings, April 23, 2009.

Bibliography

Selected Sources

Books

Bahadur, Gary, *et al.*, *Privacy Defended: Protecting Yourself Online*, Que, 2002.

A user-friendly book by network security experts explains why Internet users should care about online privacy and security.

Chander, Anupam, *et al.*, eds., *Securing Privacy in the Internet Age*, Stanford University Press, 2008.

Essays by experts in the field focus primarily on legal standards and litigation of Internet-related privacy issues.

Holtzman, David H., *Privacy Lost: How Technology is Endangering Your Privacy*, Jossey-Bass, 2006.

A former chief scientist at IBM's Internet Information Technology group covers virtually every aspect of online privacy, from the technologies that enable incursions to legal standards to the impact on personal life.

Solove, Daniel J., and Marc Rotenberg, *Information Privacy Law,* Aspen, 2003.

Coauthor Rotenberg, president of the Electronic Privacy Information Center, surveys the full range of privacy issues, not just online privacy. Includes extensive discussion of key statutes and regulations.

Articles

Burstein, Aaron J., "Amending the ECPA to Enable a Culture of Cybersecurity Research," *Harvard Journal of Law & Technology*, Vol. 22, No. 1, fall 2008.

Burstein argues there is a need to provide an exemption in the Electronic Communications Protection Act (ECPA) to allow researchers to perform cybersecurity studies and programs.

Clifford, Stephanie, "Fresh Views at Agency Overseeing Online Ads," *The New York Times*, Aug. 5, 2009, p. B1.

The article examines the pros and cons of Federal Trade Commission efforts to strengthen its oversight of online advertisers.

Griffith, Eric, "How to Reclaim Your Online Privacy," *PC World*, Feb. 1, 2009.

Griffith offers a wealth of practical tips on how to configure your computer to protect your privacy while you're on the Internet.

Kopytoff, Verne, "Paying Attention to Online Privacy: Google lawyer says the entire concept is changing as technology marches forward," *The San Francisco Chronicle*, Dec. 30, 2007, p. D1.

A lawyer for Google discusses how technology is changing peoples' views on privacy.

Studies and Reports

"FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising," Federal Trade Commission, February 2009.

The Federal Trade Commission examines behavioral targeting of online advertising as well as the advertising industry's efforts at self-regulation.

"Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress," Federal Trade Commission, May 2000.

The FTC called for legislation ensuring consumer online privacy, a call Congress has not yet answered.

"Self-regulatory Principles for Online Behavioral Advertising," American Association of Advertising Agencies, Association of National Advertisers, Council of Better Business Bureaus, Direct Marketing Association, Interactive Advertising Bureau, July 2, 2009.

While this report carries the same title as an FTC staff report that preceded it by six months, it reaches somewhat different conclusions. Specifically, the advertisers call for opt-out protections for consumers' sensitive data, while the FTC staff calls for opt-in to be required for advertisers to access sensitive data.

Dixon, Pam, "The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation," World Privacy Forum, fall 2007.

This report looks in detail at online advertisers' efforts at self-regulation and finds them wanting.

Gellman, Robert, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing," World Privacy Forum, Feb. 23, 2009.

Gellman provides a detailed discussion of the legal questions surrounding user data stored by third parties.

Landesberg, Martha K., *et al.*, "Privacy Online: A Report to Congress," Federal Trade Commission, June 1998.

The FTC's first in-depth look at online marketing and its impact on consumer privacy explores whether the advertising industry is capable of self-regulation.

Szoka, Berin, and Adam Thierer, "Online Advertising & User Privacy: Principles to Guide the Debate," Progress & Freedom Foundation, September 2008.

The authors argue in favor of behavioral targeting and recommend regulation only as a last resort.

The Next Step:

Additional Articles from Current Periodicals

Advertising

"New Tool Will Help Online Advertisers Develop Stronger Privacy Practices," States News Service, Jan. 28, 2009.

The Center for Democracy and Technology has unveiled an assessment tool to help online advertising companies develop appropriate privacy protections for users.

Cauley, Leslie, "Feel Like Someone's Watching You?" *USA Today*, Feb. 9, 2009, p. 1B.

Google and Yahoo — the two biggest players in online search advertising — say their self-imposed privacy policies provide sufficient protection for users.

Helft, Miguel, "Google to Offer Ads Based on Interests, With Privacy Rights," *The New York Times*, March 11, 2009, p. B3.

Google will begin showing ads based on users' previous online activities, but the move has drawn criticism from privacy advocates.

Puzzanghera, Jim, "Tough Cookies for Web Surfers Seeking Privacy," *Los Angeles Times*, April 19, 2008, p. B1.

Internet users can adjust browser settings to block advertisers that track user activities, but anti-Spyware programs can often negate such settings.

Puzzanghera, Jim, and Jessica Guynn, "Google, Obama May Be Clicking," *Los Angeles Times*, Jan. 24, 2009, p. A1.

Newfound political ties between Google and the Obama administration heighten concerns over data-privacy issues and its grip on the online advertising market.

Steel, Emily, "FCC Backs Web-Ad Self-Regulation," *The Wall Street Journal*, Feb. 13, 2009, p. B7.

The Federal Communications Commission (FTC) has endorsed industry self-regulation as a means of protecting consumer privacy in the online advertising market.

Federal Regulations

Ackerman, Elise, "Google Gets OK to Buy Ad Firm," *San Jose* (California) *Mercury News*, Dec. 21, 2007.

Google has won FTC approval to buy the online advertising agency DoubleClick, but such a merger could compound dilemmas over online privacy.

Ackerman, Elise, "FTC Revises Guidelines for Online Behavioral Targeting," *San Jose* (California) *Mercury News*, Feb. 12, 2009.

The FTC has introduced guidelines that would require sites to disclose the data they are collecting from users and give them the chance to opt out.

Clifford, Stephanie, "Web Privacy on the Radar in Congress," *The New York Times*, Aug. 11, 2008, p. C1.

Issues relating to data collection and Internet privacy policies are beginning to attract the attention of Congress.

Gage, Deborah, "Privacy Laws Need Better Controls, Panelists Say," *The San Francisco Chronicle*, Dec. 16, 2007, p. E1.

An advocacy group says clearer laws and better technological controls are needed over what online information can be made public.

Glass, Kat, "FTC Opts to Stay Out of Regulating Web Privacy," *Wichita* (Kansas) *Eagle*, July 10, 2008, p. A1.

The FTC has indicated it will leave it to Internet companies to decide how best to protect users' privacy.

Hansell, Saul, "Agency Skeptical of Internet Privacy Policies," *The New York Times*, Feb. 13, 2009, p. B5.

The FTC says Internet companies are not clearly explaining to users what data they collect and what it is used for.

Hart, Kim, "A New Voice in Online Privacy," *The Washington Post*, Nov. 17, 2008, p. A6.

A group of privacy lawyers, scholars and corporate officials has launched an advocacy organization calling for tougher regulations on the collection and storage of online user data.

Hsu, Spencer S., and Cecilia Kang, "U.S. Web-Tracking Plan Stirs Privacy Fears," *The Washington Post*, Aug. 11, 2009, p. A2.

The Obama administration is proposing to scale back a ban on tracking how people use government Web sites.

Kopytoff, Verne, "Rules Suggested for Tracking Internet Use," *The San Francisco Chronicle*, Feb. 13, 2009, p. C1.

Federal regulators have issued new guidelines for Internet companies that track user behavior online and use such data to tailor advertisements accordingly.

Newell, Ben, "Senate Looks at Privacy Options," *The Washington Times*, July 10, 2008, p. A9.

Sen. Byron L. Dorgan, D-N.D., is proposing a "do not track" list to prevent Internet companies from collecting personal information.

Steel, Emily, "Web Privacy Efforts Targeted," *The Wall Street Journal*, June 25, 2009, p. B10.

The possibility of new Internet privacy regulations has prompted online advertisers to give online users more control over how their information is collected and used.

Tessler, Joelle, "Microsoft, Google Back Broad Privacy Legislation," The Associated Press, July 10, 2008.

Both Microsoft and Google told Congress to pass basic privacy legislation to protect information regarding consumers' Web-surfing habits.

Smartphones

Cauley, Leslie, "FCC Taking 3-Part Look at Wireless," *USA Today*, Aug. 24, 2009, p. 4B.

The Federal Communications Commission is examining the state of the wireless communications industry in order to better address consumer privacy concerns.

Hettich, Colter, "Where's Waldo?" *Abilene* (Texas) *Reporter-News*, Feb. 9, 2009.

A new Google software program makes it possible for individuals to locate one another by using their cellphones.

Markoff, John, "You're Leaving a Digital Trail. Should You Care?" *The New York Times*, Nov. 30, 2008, p. BU1.

New technologies, such as smartphones, have become so powerful that they threaten the protection of individual privacy.

Nakashima, Ellen, "When the Phone Goes With You, Everyone Else Can Tag Along," *The Washington Post*, July 12, 2008, p. A1.

The launch of the iPhone 3G signals the augmentation of precise-location technology and online advertising.

Nathanson, Rick, "They Are Watching You," *Albuquerque (New Mexico) Journal*, June 15, 2008, p. E1.

As smartphones and other technologies become more complex, privacy becomes more and more of an illusion.

Stone, Brad, "The High Security Risk Attached to Obama's Belt," *The New York Times*, Jan. 12, 2009, p. B1.

Barack Obama has been denied the use of his BlackBerry upon taking office because of concerns over security and privacy.

Weddle, Eric, "Smile, You May Be on Someone's iPhone," *Journal and Courier* (Indiana), Sept. 3, 2009.

A student at Purdue University in Indiana has developed a smartphone application that makes it possible to view 29 Web cameras on campus.

Social Networking

Baig, Edward C., "Users: Facebook's Getting 'Grabby' With Our Data," *USA Today*, Feb. 18, 2009, p. 3B.

Facebook has introduced a clause that gives itself rights to user data even after it's been deleted.

Boudreau, John, "Facebook Adding Safeguards Against Cyber-Bullying, Porn," *San Jose* (California) *Mercury News*, May 8, 2008.

Social networking site Facebook is adding 40 safeguards to protect youths from sexual predators and cyber-bullies.

Huang, Lily, "Protect the Willfully Ignorant," *Newsweek*, March 24, 2008, p. 54.

Internet users can't make decisions about privacy in online networks if they don't know what the trade-offs are.

Kopytoff, Verne, "Facebook Tidies Up Privacy Settings," *The San Francisco Chronicle*, July 2, 2009, p. C3.

Facebook is trying to simplify methods for users to adjust their privacy settings on its site, acknowledging that the current process has become complicated.

Leber, Holly, "Facebook Users Urged to Be Cautious With Content They Post," *Chattanooga* (Tennessee) *Times Free Press*, March 3, 2009, p. E1.

Critics warn that content posted on social networking sites can fall into the wrong hands, regardless of whether people have been classified as "friends" on such sites.

Regan, Tom, "Facebook Faces Up to Privacy Concerns — Again," *The Christian Science Monitor*, Dec. 12, 2007, p. 16.

A new Facebook application allows users to be informed about the Web-surfing habits of their "friends."

Stone, Brad, and Robbie Brown, "Web of Risks," *Newsweek*, Aug. 21, 2006, p. 76.

Students adore social networking sites such as MySpace, but indiscreet postings and a lack of privacy can cause trouble.

Wong, Wailin, "Web Footprints Leave Easy Trail," *Chicago Tribune*, Dec. 25, 2008, p. A35.

Social networking sites are allowing users to take their profile data to other places on the Internet, putting at stake their private data and reputations.

CITING *CQ RESEARCHER*

Sample formats for citing these reports in a bibliography include the ones listed below. Preferred styles and formats vary, so please check with your instructor or professor.

MLA STYLE

Jost, Kenneth. "Rethinking the Death Penalty." CQ Researcher 16 Nov. 2001: 945-68.

APA STYLE

Jost, K. (2001, November 16). Rethinking the death penalty. *CQ Researcher, 11*, 945-968.

CHICAGO STYLE

Jost, Kenneth. "Rethinking the Death Penalty." *CQ Researcher*, November 16, 2001, 945-968.

In-depth Reports on Issues in the News

Are you writing a paper?

Need backup for a debate?

Want to become an expert on an issue?

For more than 80 years, students have turned to *CQ Researcher* for in-depth reporting on issues in the news. Reports on a full range of political and social issues are now available. Following is a selection of recent reports:

Civil Liberties
Human Rights Issues, 10/09
Closing Guantánamo, 2/09
Affirmative Action, 10/08
Gay Marriage Showdowns, 9/08
America's Border Fence, 9/08
Immigration Debate, 2/08

Crime/Law
Interrogating the CIA, 9/09
Examining Forensics, 7/09
Legalizing Marijuana, 6/09
Wrongful Convictions, 4/09

Education
Reading Crisis? 2/08
Discipline in Schools, 2/08
Student Aid, 1/08

Environment/Society
Conspiracy Theories, 10/09
Human Spaceflight, 10/09
Gays in the Military, 9/09
Energy and Climate, 7/09
Future of Books, 5/09
Hate Groups, 5/09
Future of Journalism, 3/09

Health/Safety
Medication Abuse, 10/09
Nuclear Disarmament, 10/09
Health-Care Reform, 8/09
Straining the Safety Net, 7/09
Treating Depression, 6/09
Reproductive Ethics, 5/09

Politics/Economy
State Budget Crisis, 9/09
Business Bankruptcy, 4/09
Future of the GOP, 3/09
Middle-Class Squeeze, 3/09

Upcoming Reports

Women in the Military, 11/13/09 | Value of a College Education, 11/20/09 | Prisoner Reentry, 12/4/09

ACCESS

CQ Researcher is available in print and online. For access, visit your library or www.cqresearcher.com.

STAY CURRENT

To receive notice of upcoming *CQ Researcher* reports, or learn more about *CQ Researcher* products, subscribe to the free e-mail newsletters, *CQ Researcher Alert!* and *CQ Researcher News*: http://cqpress.com/newsletters.

PURCHASE

To purchase a *CQ Researcher* report in print or electronic format (PDF), visit www.cqpress.com or call 866-427-7737. Single reports start at $15. Bulk purchase discounts and electronic-rights licensing are also available.

SUBSCRIBE

Annual full-service *CQ Researcher* subscriptions—including 44 reports a year, monthly index updates, and a bound volume—start at $803. Add $25 for domestic postage.

CQ Researcher Online offers a backfile from 1991 and a number of tools to simplify research. For pricing information, call 800-834-9020, ext. 1906, or e-mail librarysales@cqpress.com.