CONSUMER ACTION NEWS

www.consumer-action.org • Summer 2010

Consumer Action
221 Main Street, Suite 480
San Francisco, CA 94105

Non-Profit Org.
U.S. Postage
PAID
San Francisco, CA
Permit # 10402

Change Service Requested

Online, data control is crucial

Permission before sharing, say polltakers

By Ruth Susswein

Ask before taking—this is what consumers want companies to do when dealing with personal information online. More than nine out of 10 respondents (92%) to Consumer Action's Online Privacy poll said that companies should be required to get your permission before sharing any information collected about you.

Consumers who gave detailed responses were primarily concerned that personally identifiable information should not be shared without permission. Many specified that they did not want their names, addresses, cell or phone numbers, email addresses, incomes, Social Security numbers (SSNs), bank accounts, credit card numbers, medical histories, birth dates, access codes, ages, details about their children or "any information that can be linked to me" collected or used without their consent.

In addition, 95.5% do not want their information stored, shared or sold to third parties unless the information is not identifiable. One

See "Control," page 5

Consumer Action 39th Anniversary

Senator Ellen Corbett accepts a Consumer Excellence Award from Executive Director Ken McEldowney (Ricardo Perez photo). Read more on page 6.

Bullseye: How companies target you on the Internet

By Michelle De Mooy

If the Internet is a vast sea of information, awash with consumers surfing small, specific waves of data, online advertising is like a wind machine, propelling us towards one crest or another.

Online behavioral advertising is a wind machine on steroids, keeping track of every single drop of water you touch and depositing those drops into a separate, private ocean. For online businesses that depend on advertising revenue to stay afloat, like Google or Facebook, those drops quickly are converted into gold.

Behavioral advertising, also called "behavioral targeting," is the term used to describe the practice of tailoring advertisements to an individual's personal interests based on their online activities. Unbeknownst to many consumers, companies routinely monitor online searches, website visits, specific pages viewed, geographical location (from mobile devices), purchases made or even considered, posts and updates on social networking sites, and in some cases, even emails written and received.

Behavioral advertising means you and your friends might see vastly different ads while visiting the same website. It also means that information that you might have considered anonymous or unrelated, such as search terms you typed into Google one minute and an article you read on People.com the next, are now correlated, collected, stored, and used to target you with specific offers. Sometimes this information is then combined with public data, such as demographic information like age and gender, and used to create a detailed profile of you.

Behavioral targeting is rapidly becoming difficult to avoid on the Internet. Companies are spending millions of dollars on this practice because they believe it turns cyber window shoppers into buyers. Many online services and sites, like search engines or social networking sites, are free to users because companies earn their income by selling advertising. They use behavioral advertising because it's believed that targeted ads generate more sales and more revenue.

Cookies: Not so sweet

Behavioral advertising begins when ad networks store and track "cookies"

See "Target," page 5

Fans don't 'like' Facebook's very public privacy misstep

Attention has been focused on Facebook, the social networking giant with over 400 million users around the globe, since the company came under fire for substantial, unilateral changes it made to its privacy policy.

Consumer and privacy advocates, including Consumer Action, were outraged by some of these changes. Key among the concerns was Facebook's decision to switch some non-public information (such as items designated for "Friends Only") to public status (or "Everyone") for all users without their consent. The new default settings also disclosed personal information, such as game applications, to third parties, that previously had not been public.

The company claimed to be operating within new "social norms" that indicate people are more willing to publicly share their personal information online. Many Facebook users disagreed with this assessment and felt the company was disregarding their very real privacy concerns.

The Electronic Information Privacy Center (EPIC), along with 12 other consumer organizations, filed a complaint in December with the Federal Trade Commission (FTC), claiming that Facebook engaged in "unfair and deceptive trade practices" by making these changes. Among other things, the EPIC complaint accused Facebook of making material changes to its privacy settings in violation of user expectations, and stated that the new policies directly contradicted the company's former privacy policies.

The FTC has yet to comment on the complaint but says it plans to release new guidelines for social networking companies by the end of the year.

As a result of pressure from advocates, users, and Congress, Facebook released a privacy revamp that included a new, cleaner look for its privacy settings, an option to "opt-out" of all third party sharing of information, and more user control over information. Given an advanced preview of the new settings, Consumer Action provided Facebook with feedback on the changes and urged the company to go further to protect users' privacy.

"With these changes, Facebook appears to be committed to improving user access and control of their privacy settings, and increasing their ability to opt-out of information sharing," said Michelle De Mooy, senior associate for national priorities at Consumer Action.

"But it needs to do more. First and foremost, Facebook should commit

See "Facebook," page 8

About this issue

This issue of *Consumer Action News* was funded by our Privacy Information Project (www.privacy-information.org).

Privacy Information
A Consumer Action Project

Consumer Action

www.consumer-action.org

Consumer Action has been a champion of consumers nationwide since 1971. A nonprofit 501(c)3 organization, Consumer Action focuses on financial education that empowers low to moderate income and limited-English-speaking consumers to financially prosper. It also advocates for consumers in the media and before lawmakers to advance consumer rights and promote industry-wide change.

By providing financial education materials in multiple languages, a free national referral and advice hotline, and detailed pricing surveys, Consumer Action helps consumers assert their rights in the marketplace and make financially savvy choices.

Consumer Action provides nonlegal advice and referrals on consumer problems. Chinese, English and Spanish are spoken. Call or write:

(415) 777-9635 • (213) 624-8327

hotline@consumer-action.org

Consumer Action News is printed by the Dakota Printing Company, using recycled paper and soy-based ink.

In 'cloud,' your privacy could hit some rough weather

By Linda Sherry

What is "cloud computing?" You are using cloud computing services when you use web-based email, share news on your Facebook page, upload family photos to Flickr, display your videos on YouTube, back up your computer with Norton Online, use iCal to keep your appointments, collaborate on files using Google Docs, pay your bills on your bank's website, or look for a mate on Match.com.

With these and a myriad of other cloud-based services, you store your electronic data (emails, documents, photos, music, video, credit card numbers and other information about yourself) on remote servers. This vast network of servers, storage systems, and devices is what makes up the "cloud." Basically, the "cloud" is "cyberspace."

In most cases, cloud computing uses your browser and web-based software to communicate, work and play, rather than software you install and run directly on your own computer, such as a word processing program, photo editing software or video game.

A September 2008 poll by the Pew Internet & American Life Project found that 69% of people in the U.S. who access the Internet used some form of cloud computing, from web mail, online photo or video storage, to web-based applications that store data on servers, instead of on personal computers.

In the past several years, the use of cloud-based services has grown by leaps and bounds. In the cloud, you cannot only store data, images and documents; you can create, edit, manipulate and share them.

But how safe is the cloud? How private is the cloud? A lot of the stuff we are storing and sharing on the Internet is personal, confidential or sensitive in nature. Most individuals want control over their personal information, but users of the cloud rely heavily on data and software they don't own or control.

Fortunately, many companies used to storing sensitive data in the cloud—such as financial or health records—are hyper-vigilant about user privacy. Your accounts are password protected and the information typically is transmitted over secure servers. (Look for the S in "https//: in your browser address window to ensure you are using a secure channel.)

But the growth of cloud computing raises privacy and security concerns that go beyond secure access and storage. A server (or a huge group of servers called a server "farm") by its very nature can be established anywhere on earth. U.S. consumers who upload photos might be sending them to a server farm in Kansas—or one in Russia. Is the data stored in the USA and subject to U.S. law—or it is stored in Russia and subject to that country's laws? This is still an unanswered question.

Bob Gellman, a privacy consultant, points out many privacy and security concerns about the cloud in a paper released late last year. He believes that "consumers are too cavalier when using most Internet services, and that includes cloud computing."

According to Gellman, "Consumers allow providers to collect, compile, use, and sell their personal information, even when it would not be hard for consumers to protect their data by using a different search engine, telling their browser to erase cookies, or changing their IP address." He says most consumers can limit the data collected about them by turning off their routers for one minute and then turning them back on, which changes the IP address.

Gellman advises caution about what you store on remote servers outside your control. "Don't put anything in the cloud you would not want the government or a private litigant to see."

(Linda Sherry photo)

Benefits of the cloud

Consumers who use cloud-computing services may be attracted by the many benefits. You don't have to worry about losing data when your hard drive crashes or your laptop is stolen if you have it backed up in the cloud.

In the cloud, your data is portable, and you can access it from any computer or communications device with wireless connectivity. You can share large files (photos, movies and video) that cannot be sent by email.

You can collaborate on documents and communicate with others regardless of the distance between you.

Some medical providers are enthused about the ability to share your electronic health records with each other and to ensure that your care is coordinated. Google and Microsoft have created cloud-based "personal health records" (PHRs) in which you can upload your medical records and other health-related information about yourself and share them, if you wish to. These PHRs can upload data from home health devices such as scales, insulin monitors and blood pressure cuffs, and the data can be stored in your PHR.

Threats in the cloud

Cloud computing services store business records, resumes, medical records, and many other sensitive documents. Before you upload or keep your information on a remote server, make sure you understand how the site can use your information. Can they sell it? Can they "share" it? What other companies can access it for routine business needs?

Start by reading the privacy policy, but also ask yourself, "What could happen if this information got out to people I don't want to have it?" This question is especially crucial when it's asked about sensitive medical information.

Many people forget to consider what will happen to the information they store or backup online if the company they use goes out of business. Another concern is when a new company buys your provider—you can't really be sure that the new owner will honor your original provider's privacy, security and data use policies.

Many jobseekers post resumes on job-hunting sites, where potential employers can download them. Does your resume contain personal information you'd rather keep private? Pam Dixon of the World Privacy Forum suggests that you post your resume "privately" on job sites.

"It's not just employers that access your resume on resume databases," Dixon notes. "Criminals and fraudsters posing as recruiters can gain illicit access to resume databases, among others."

Privacy policies on reputable sites should explain how the company limits its secondary use of data. But there are certain things even vigilant companies have trouble guarding against, such as malicious employees. Employees with an axe to grind, or who are bent on committing identity theft, are a weak link in data security.

Security breaches and account highjacking can happen from the outside, too. Sophisticated hackers can wreak havoc by stealing data—including credit card numbers stored on websites—and use the information to commit fraud or even just to cause trouble and embarrassment for a company.

Law enforcement authorities—with a subpoena—can probably obtain anything you store on a remote server. According to the ACLU, courts have yet to definitively determine how traditional privacy protections apply to cloud computing documents.

Fred von Lohmann, a senior staff attorney with the Electronic Frontier Foundation, noted on the group's website: "Remember that the feds could ask Google for your search history. And so can any private litigant with an axe to grind and a subpoena in hand. If someone does deliver a subpoena to Google for your records, there is no law that requires that you even be notified, much less be afforded an opportunity to object." ■

Further reading

Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, Bob Gellman, World Privacy Forum, www.worldprivacyforum.org

Cloud Computing: Storm Warning for Privacy, Nicole Ozer, ACLU, dotrights.org

A privacy generation gap?

By Ruth Susswein

Is there a "privacy gulf" between generations? Do you and your children disagree on how much personal information should be shared online?

Based on the carefree approach to online networking among tech-savvy Millennials— youth born and raised in the digital world—many have suggested that young people don't care about defending their privacy online.

Not true, according to an April study, that says that young adults are no less concerned about protecting their privacy than older online users.

The survey by the University of California-Berkeley and the University of Pennsylvania, found that the vast majority of 18-24 year olds surveyed were "in harmony with older Americans regarding concerns about online privacy."

Young adults told surveyors:

• Websites should be required to let people know whatever information the site has about them.

• There should be a law requiring websites to delete all stored information about an individual.

• Anyone who uploads a photo of her or him to the Internet should get permission first, even if the photo was taken in public.

These results were very similar to what the study found with older adults. The study's authors attribute some young adults' more privacy-casual online personas to a lack of privacy knowledge.

Close to half (42%) of the young adults who took a five-question privacy quiz as part of the study got *all* the answers wrong. The authors concluded that young adults do not lack concern about privacy matters in a "tempting" online environment; they lack knowledge.

Misleading privacy policies

Study co-author Chris Hoofnagle of UC Berkeley's School of Law attributes the perception to the existence of so-called privacy policies.

Hoofnagle believes that people mistakenly conclude that if a company has a privacy policy, it means your information will remain private.

"If you call it a privacy policy it should have some privacy in it," says Hoofnagle. But instead he says these policies often are merely "information use statements." He argues that, among other things, real privacy policies should prohibit the sale of your information to third parties.

The study is titled "How Different Are Young Adults from Older Adults When it Comes to Information Privacy Attitudes & Policy?" To find the full text, do an online search using the words "Hoofnagle and young adults". ■

A principled approach to online privacy protection

Leading consumer and privacy groups have developed privacy principles to protect consumers on the Internet, while still allowing for robust online commerce. These principles have been recommended to Congress as the basis for privacy legislation. Consumer Action is a member of the Privacy Coalition that supports these principles:

Relevant data collection

• No behavioral data about children under 18 years old should be collected or used.

• Personal and behavioral data collected should be relevant to the purposes for which they are to be used.

• Limits should be placed on how much personal and behavioral data are collected, and where appropriate, consumers should be notified and consent to data retention and any other unrelated uses of their data.

• Sensitive information should not be collected or used to track or target customers. Sensitive data would include information about one's health, financial, ethnic, racial, sexual orientation, personal relationships, and political activity.

• The reason that personal and behavioral data is being collected should be explained in advance, and should be used only for the purpose given. If the reason changes, consumers should be given the right to refuse the use or further collection of their information.

• Information about people should be protected whenever their profiles can be linked to a particular computer, even when their names, addresses or other identifiable information are not revealed.

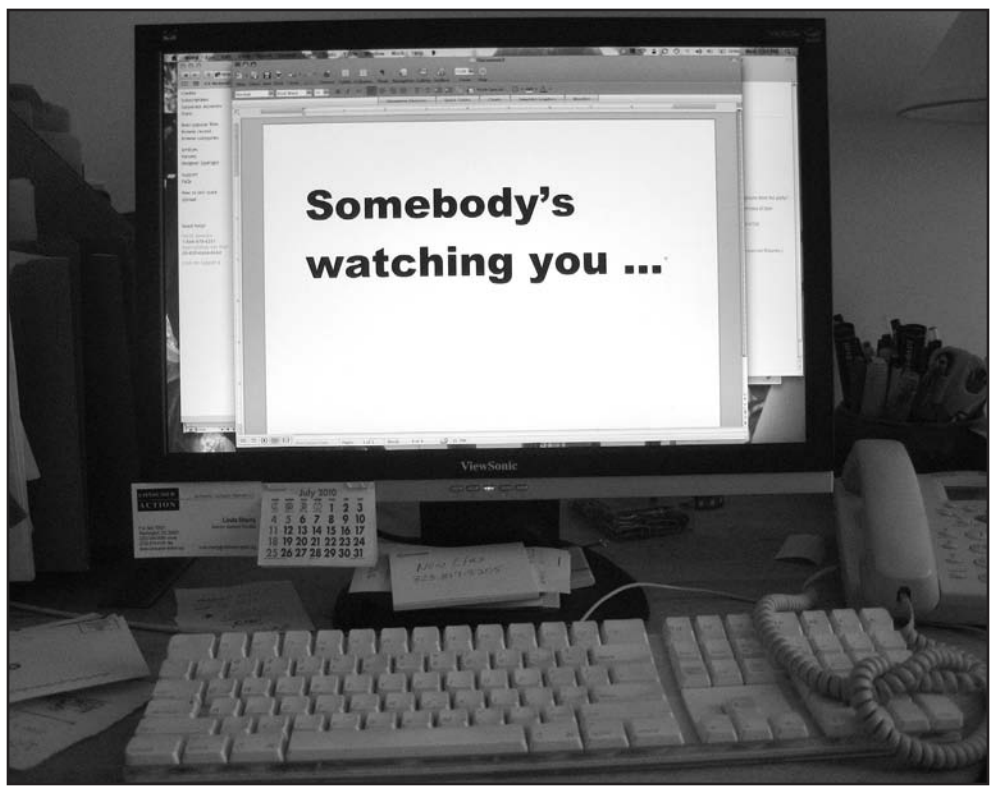
• Websites and networks should not be able to collect or use behavioral information for more than 24 hours without a consumer's express consent.

• The highest standards should be used to safeguard collected personal data from theft, loss, unauthorized access and modification.

Consumer access

• Consumers always should be able to see the personal and behavioral information about them that is being stored by behavioral marketing or advertising companies. Individuals should have the right to see and verify their personal information in a timely manner and, if they are charged, for a reasonable fee.

• If denied access to information collected about themselves, consumers should have the right to challenge the denial and have personal information changed or erased. ■



Online privacy protection is no joke *(Linda Sherry photo)*

Six great tips to protect your privacy while you're online

By Ruth Susswein

We've compiled some of the best advice from top privacy experts to help you protect your personal information online.

Here's what they recommend:

Beth Givens, director, Privacy Rights Clearinghouse: It's a good idea to avoid using the same website for both your web-based email and as your searches on the Internet. Your web mail account will always require some type of a login, so if you use the same site as your searches, they can be connected to your email account. By using different websites for different needs—perhaps Yahoo for your email and Google for your searches—you can limit the information retained by any one site.

Rainey Reitman, privacy advocate, Privacy Rights Clearinghouse: Job seekers beware! Companies routinely review information posted on social networking sites when hiring. Ask yourself, would you be comfortable if the photos and personal information you've posted online were made public? Do you really want your boss (or your mother) to see it?

For more, see the Privacy Rights Clearinghouse "Social Networking Guide," at www.privacyrights.org/social-networking-privacy.

Pam Dixon, executive director, World Privacy Forum: Use a "throw away" email address (not your permanent one) when using search engines (Google, Bing etc.) so that third parties can't link all sorts of information to you. Mix it up – use various search engines when online, and don't include your full name with other key information (such as passwords) that could be stored about you. Be most careful when using your iPhone or Blackberry online with programs that link to your social network, called "third party applications." You are much less anonymous on a phone. Each phone has a unique identifier and could connect you to your online posts, such as those negative comments you wrote about your employer.

See "Search Engine Privacy Tips" at www.worldprivacyforum.org/searchengineprivacytips.

Bob Gellman, privacy consultant: If you're not engaging in a financial transaction online, then lie! You can say whatever you want. I often play "spin the box." Whenever I'm given a box with choices to identify myself, I give random answers. Once I was 7-year-old Serbo-Croatian dentist. If you have access to your router, you can turn it off for one minute and that will (often, not always) erase the cookies connected to your computer.

Linda Sherry, director of national priorities, Consumer Action: Manage your "cookies" carefully. Cookies are tracking links that companies download onto your computer. Check the Help section of your browser (Firefox, Internet Explorer, etc.) on how to block or delete cookies. Cookie control settings can be found in the Preferences section of your browser.

Sherry also suggests using your browser's "private browsing" setting or a website such as Anonymizer.com if you do not want to be tracked.

Chris Hoofnagle, director, UC Berkeley School of Law, Center for Law and Technology: Use a new, free browser add-on at www.Abine.com that blocks many network tracking cookies and downgrades cookies it cannot block from permanent to per-session status. So when you turn your computer off, the cookie disappears which means your information is no longer available to others to share, sell or store.

"It will also block web bugs and help you generate better user passwords when shopping online. It will suggest a user password for you," says Hoofnagle. He's tested the program and finds it quite effective without causing connection difficulties for sites you choose to visit—a problem that can sometimes occur when cookies are deleted.

Overall, it is important to realize that no amount of detection and prevention will fully protect your privacy, but limiting the information you share and disconnecting these cybersponges will help you control access to your personal information. ■

Sensitive info may not be as protected as you think

By Michelle De Mooy

From birth to old age, medical records can be a map of our lives, detailing great joys and great sorrows alongside everyday bumps and bruises. They are often the most private and vulnerable pieces of information that exist about us. What happens when these records, once limited to the physical confines of your doctor's dusty filing cabinet, get a digital life of their own?

Electronic medical records have been used for much of the last 20 years. Doctor's offices, hospitals, and health insurers regularly use some form of digital medical records, whether to enter your lab test results into a hospital databases or to access electronic files with details about your latest insurance reimbursements.

Though technological innovations have increased the ability of these entities to treat, diagnose, track, store and collect medical information about you, federal law has yet to comprehensively protect the privacy and security of these records as they pass through more and more hands.

Much of your medical information is already routinely shared, legally, without your knowledge.

A wide range of people, including your primary care physician, specialists, health insurance employees, and business associates of health care systems, are allowed to access to your private medical records.

Two pieces of legislation govern much of how patient privacy is handled today:

• The Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress in 1996 to set a national standard for electronic transfers of health data.

• The HIPPA Privacy Rule was created by the U.S. Department of Health and Human Services in 2003 to address the privacy and security of personal health data itself.

Both laws provide fundamental aspects of patient privacy, such as the ability to access your own medical records, but do little to keep this information between you and your doctor.

Under these statutes, your private health information can be used for marketing purposes and your doctor may disclose details about your medical condition to a "business associate," such as a debt collector, without your knowledge or consent.

More patient control

Despite privacy drawbacks, studies have shown that electronic records have many benefits, including reduction in medical errors and overall costs for providers and patients. During his campaign for president, Barrack Obama pledged to work toward achieving these benefits for Americans by implementing a comprehensive health technology (health IT) system. In February of 2009, he lived up to his promise with the passage of the American Recovery and Reinvestment Act, which will create a system of electronic health records by 2014.

Many consumer and privacy advocates, including Consumer Action, worked with legislators to make sure the Act included significant improvements in health privacy. Some of the improvements include more transparency in the lists of who has seen and used your medical data (audit trails), and stiffer penalties for violations of patient privacy.

The law also prohibits the unauthorized sale of personal health information (PHI) (with some exceptions for medical research), limits the ability of marketers to see and use PHI, and gives individuals the ability to prohibit disclosure of their information.

Monitoring your records

As health IT rolls out in next few years, it will become more important for consumers to pay close attention to the information contained in their medical records as well as who is accessing them.

You have the right, under HIPAA, to view the original records, make corrections if necessary, and obtain copies in a reasonable timeframe. Many doctors' offices have a policy regarding how long it will take to receive copies of your records, and there's usually a copying fee. Though it's not necessary to make a written request, Consumer Action suggests you send a letter so that you'll have a paper trail if you run into trouble.

If you have trouble accessing your records or getting copies, you can complain to the Department of Health and Human Service's Office of Civil Rights at 200 Independence Ave. SW, Washington, D.C. 20201. Call 866-627-7748 or visit www.hhs.gov to learn more.

Depending where you live, you may have the right to complain to state regulators if your rights are violated. Google the Georgetown University Center on Medical Record Rights and Privacy website to get a state-by-state guide on medical privacy laws.

So far, it appears there is no legal distinction between paper and electronic medical records. Records must be kept in an unaltered form and authenticated, usually by the health care provider. Technically, the provider owns the records.

Despite the unfortunate reality that patients are not in full control of their medical information, there are a few ways you can stem the flood of your data.

Keep an eye on your records. HIPPA gives patients a right to review their own records. This is an important way to keep track of where your information might be flowing, such as to a specialist for a second opinion or to a local pharmacy to fill a prescription. If you have questions about something in your records, ask your doctor or health care provider.

Address mistakes. If you find any errors on your records, it's important to take the time to correct them. You can do this by making a request—in writing—to the office that made the mistake. Make sure to keep a copy.

Be the squeaky wheel. Though consumers do not have the right to sue for privacy violations under HIPPA, you do have the right to complain. You should receive written notice from your health care provider that details how to do this.

If you don't receive a response, you can file a complaint with the Department of Health and Human Services within 180 days. Remember, you cannot be denied treatment or care for filing a complaint. ■

Legislating privacy

By Michelle De Mooy

Safeguards for online privacy in America could change dramatically this year if proposed legislation aimed at protecting the privacy of data online gains traction. Representative Rick Boucher (D-VA), chairman of the House Subcommittee on Communications, Technology, and the Internet, unveiled a draft bill in May.

Though the bill offers some protections to consumers, such as requiring companies that collect personal information online to provide a clear and conspicuous privacy policy that details how data is collected and used, many advocates view the bill as weak and far from consumer-friendly.

Among other concerns, the bill mimics current industry practices by making consumers "opt-out" of, or turn off, automatic data collection. However, even this approach would not be required for companies to collect what's deemed "operational" or "transactional" user data, which would include standard records such as Web logs or cookies (digital records of an individual's activities as they surf).

Also, the legislation would override stronger state consumer privacy laws, meaning it would actually place fewer restrictions on companies which collect, use, and disclose consumer data. While companies collecting and using "sensitive," information, such as health and financial information, would be obliged to get an "opt-in," or express permission from consumers, the bill mostly exempts the more notorious data purveyors from this requirement—third party ad networks. Ad networks, such as BlueKai, purchase advertising space from websites and then monitor consumer behavior online in order to target ads to them.

Some industry representatives have opposed many parts of the privacy bill as being too strong. Businesses particularly don't like that the bill proposes to place a limit of 18 months on how long companies can hold and use data.

Consumer Action joined advocates in calling for stronger provisions in the bill, including:

• No override of state laws (preemption).

• Citizens' rights to sue companies for privacy violations.

• Limits on the amount of data collected.

Many consumer protections are being decided in the 111th Congress. (Linda Sherry photo)

• Shorter, stronger limits on how long companies can store personal data.

• Public notice for security or data breaches.

• The creation of a consumer complaint database.

Pam Dixon of the World Privacy Forum says that the privacy bill relies on a weak opt-out process that is too technical, requires a separate download, and is too hard for most consumers to understand and use.

In 2007, the World Privacy Forum spearheaded a proposal for a "Do Not Track" list, similar to the national "Do Not Call" phone list, which would empower consumers to restrict companies from tracking which websites they visit.

In May, Consumer Action joined other groups in submitting comments to Rep. Boucher. Negotiations are expected to continue throughout the summer.

The privacy bill is likely to evolve and change in the coming months, keeping the already boiling issue of online privacy right on the nation's front burner. Stay tuned! ■

Control

Continued from page 1

responded that "it would be ok to disclose my pattern of activity" but many wanted online businesses to obtain their consent before storing or sharing any personal information.

Most consumers (78%) say that they are not comfortable being tracked online. In fact, nearly three quarters of respondents (70%) feel that online tracking is a violation of their privacy, and close to 25% more sometimes call it a privacy violation.

"Consumers are resolute in their demand that companies seek their permission before sharing, selling or storing information that can be linked to an individual," says Linda Sherry, Consumer Action's director of national priorities. "Our survey results confirm that consumers overwhelmingly support opt-in privacy policies."

Privacy policies

The survey also ask how consumers view website privacy policies.

When asked, "When you visit a website do you read the privacy policy?" 47% said they do not read the policy; 46% said they sometimes read the policy.

In fact, close to half of those surveyed (44%) noticed privacy policies only some of the time.

Of those who had taken the time to read some policies, we asked, "What do you look for in a privacy policy?" Most people told Consumer Action that they want to know exactly what information is being collected about them, what information is shared or sold, and whom it will be shared with.

Some consumers say they look for limits on information sharing, while others seek assurances that their information is not being shared or sold at all. Some try to gauge how the company keeps collected information secure. Some look for what's not in the policy.

While some respondents say they just "don't care enough," many said they didn't have the time to read policies, or to opt-out each time they visit a new site. Others called the privacy policies too "generic," "vague," "too long" and too "technical." Some say the "policies are for companies, not consumers." Still others say, "I accept that they will invade my privacy," or call the guidelines "irrelevant, there is no privacy on the Internet."

More than 97% of those surveyed say that companies track you online to try to sell you something. 15% also said companies track you to ensure that you don't download copyrighted material. Nearly 40% believe that companies track every single move you make, while more than half (55%) say they're tracked but not by every single move.

The majority (76%) have heard of behavioral advertising, and 65% believe that it is online advertisers who track users to see what they might be interested in buying, and that you are shown ads based on what you look at online, your Facebook friends and email messages.

But are they buying products that online advertisers are pitching? No—only about 19% of those who clicked on ads have made a purchase, while 81% have not.

Opting out

Survey results show that industry is not doing all it can to educate consumers about their ability to control some targeted advertising. About 90% of polltakers did not know that Google, Yahoo, and the trade group the Interactive Advertising Bureau allow you to opt out of receiving behavioral ads. More than half (57%) of the respondents are Facebook members. Another 7% said they had been members but they quit, mostly because of privacy concerns.

Most participants (68%) believe that Internet advertisers have easy access to your online history ("cookies" and IP addresses), but more than half (52%) say that your name and address are also accessible. A full third of those surveyed (34%) say that your credit card number and your SSN can also be easily obtained.

Generally, the correct answer to the question "What information can online advertisers easily obtain" is your online history. While financial and personal information can be accessed too, it would require more effort and multiple data sources to accomplish. (The percentages do not add up to 100 because multiple answers were accepted on this question.)

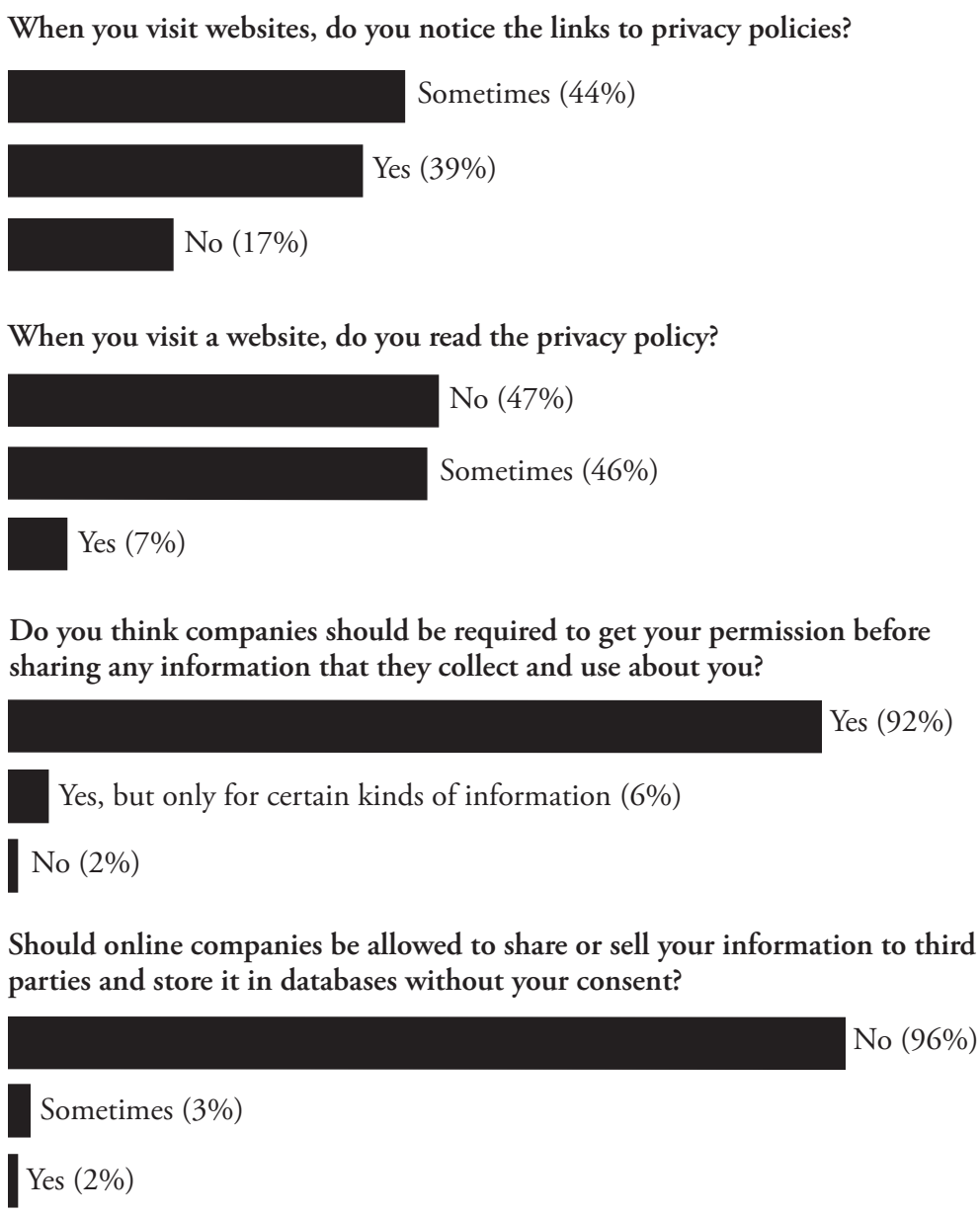
"Most people got this one right, but since a third of respondents believe that most other information is also readily available, like credit card and Social Security numbers, that may explain part of the reason why an overwhelming majority insists on consumer consent before data is shared," says Sherry.

Consumer Action conducted its survey of consumers' online privacy preferences from June 15-30 using Survey Monkey (www.surveymonkey.com). 762 consumers participated in the survey online.

The survey was publicized through Consumer Action's website and promoted by email to our network of community-based organizations, online members, Take Action Center subscribers, people who had lodged complaints with us, and privacy and consumer affairs listservs. ■

Online privacy attitudes

This chart highlights four telling responses from Consumer Action's survey of consumer attitudes about online privacy preferences. Overall, 762 individuals participated in the survey. (Percentages have been rounded to nearest number.)



Target

Continued from page 1

on your computer.

Cookies are digital bits of information about you. Cookies are assigned to you (by a network's web server) without your knowledge as you surf the web. They keep a digital memory of your online patterns and preferences, such as websites you've visited and shopping carts you've filled, as well as passwords and usernames you've chosen. (You can decide whether your passwords and usernames are stored in your browser, but don't click "remember" for your bank and other sites that store confidential information.)

The information stored on cookies can be used to build a profile of you, which ultimately may be used to target you with specific ads. For example, if you filled out an online form to receive a trial magazine subscription, which asked for your name and address, this information could be stored in a cookie.

There are two kinds of cookies. "First party" cookies are used only by the company you do business with, which might then send you coupons or other targeted ads when you return to the site. Cookies that send your data elsewhere are called "third party." Some third party cookies, for example, route your information to advertising clearinghouses, which then sell information about you to other marketers.

Every click you make

So how much do companies actually know about you? According to groups like the Network Advertising Initiative (NAI), an industry trade group that develops self-regulatory standards for online advertising, or the Interactive Advertising Bureau (IAB), another industry trade group representing online advertisers, the information companies have is minimal, scattered in different databases, and not identifiable, meaning it can't be traced back to an individual.

But if you ask privacy advocates, like Jeff Chester of the Center for Digital Democracy, advertisers know a lot more than that.

"Madison Avenue and Silicon Valley have merged forces to create what it calls an online marketing ecosystem. Every move one makes on and even offline is collected, stored, and deployed to target a consumer—whether they are in front of a PC, using a mobile phone, or even while playing an online video game," says Chester.

Gaining control

You can control some ways in which companies target and track you online. For example, it's possible to detect and delete first and third party cookies via settings in your web browser or by using specially designed software to route them out. You can also opt-out of sharing cookie data with members of the NAI by visiting www.networkadvertising.org.

Because of public backlash over behavioral advertising, some online businesses like Google and Yahoo! have begun to offer consumers the ability to "opt-out" of some behavioral advertising and manage a list of advertising categories to determine which ads they deliver to you. Some companies have also begun allowing users to view what information companies have about them. For example, they might show transcripts of online chats, a list of files sent and received, and copies of online documents.

Tips

To gain *some* measure of control over who sees data about you and your online habits:

- Choose to opt-out of behavioral advertising when possible.
- Use different companies for different web-based activities, like email and searches.
- Limit how much information you supply to any one company.
- Be wary of downloading any software that includes a desktop "toolbar," which are usually designed to assign cookies and other tracking mechanisms to your computer. ■

Celebrating Consumer Action at age 39

By Joe Orozco

Consumer Action's anniversary party in San Francisco was marked by spirited mingling among supporters and fellow advocates, whose generosity raised close to $50,000 for our financial empowerment activities.

The event, held in late June at the Parc 55 hotel in San Francisco, marked the 39th anniversary of Consumer Action's advocacy and education work.

As always, a highlight of the evening was the presentation of Consumer Action's Consumer Excellence Awards. This year's awardees were California Senator Ellen M. Corbett (D-San Leandro), KTSF Chinese News, and the Public Justice public interest law organization.

"It's been another banner year for Consumer Action," said Executive Director Ken McEldowney. "Our outreach team has forged new partnerships with community-based organizations, our DC office has been in the front ranks fighting for national privacy rights, health insurance rights and financial reform, and our administrators continue to keep our engine tuned for instant acceleration."

McEldowney thanked supporters for the funding that allows Consumer Action to create and distribute its quarterly newsletter and run its free, multilingual consumer assistance and referral hotline.

The Consumer Excellence Awards have been a tradition with Consumer Action for two decades, noted McEldowney.

"The mission of Consumer Action could not be fulfilled without the collaboration of key partners," he said. "This year's awardees represent media and advocacy organizations that have proven their commitment to important consumer issues in California and across the U.S."

Senator Ellen Corbett

The 2010 Consumer Excellence Award for Outstanding Advocacy was awarded to Senator Corbett, who throughout her legislative career has proven to be one of the strongest defenders of the rights of California's consumers. Last year, Senator Corbett put a priority on the passage of the Car Buyers Protection Act, which provided additional protections for people who purchase or trade in vehicles.

The Senator, a Democrat, is currently working on legislation to inform tenants of their rights during home foreclosures as well as to protect such tenants' rental histories. Corbett also leads efforts to protect children's privacy while using social networks. Other issues of concern to the Senator include consumer-friendly prescription labels, enforcing toxic toy safety laws, and the ability for consumers to get cash in exchange for gift cards with low balances.

"From banking to housing, product safety to healthcare, personal privacy and environmental protection, I have been so lucky to work on so many issues and so lucky to have been able to work with people like you," Senator Corbett told the crowd. "For almost 40 years, Consumer Action has led the fight to enact tough laws to protect people in all walks of life and has made sure that consumers know and exercise their rights."

KTSF Chinese News

In our media category, Consumer Action recognized KTSF, a widely viewed Chinese-language news station broadcasting in the San Francisco Bay Area. KTSF founder Lillian Lincoln Howell launched the station in 1976 with the mission of "serving the underserved." To reach this goal, KTSF hired experienced Chinese broadcast journalists to achieve the highest journalistic standards. Over the past two decades, the KTSF Chinese News has contributed to the community it serves with hard-hitting consumer news stories, such as its recent stories on selling personal jewelry, new credit card laws and Internet safety. KTSF coverage has helped Consumer Action reach consumers in the Chinese-American community and to help them become savvy consumers.

Rose Shirinian, KTSF news director, accepted the award. "KTSF serves the Bay Area's multicultural communities in over 12 different languages," said Shirinian. "But we can't do it without partners and we rely very much on the partnership we've had with Consumer Action for so many years."

"When we started the Cantonese news in 1989 and the Mandarin version in 1991, Consumer Action was there to help us in bringing vital information to our consumers and to our viewers," said Shirinian.

Public Justice

Public Justice was the recipient of our award in the area of Outstanding Community Service. Among other accomplishments, the dedicated public interest lawyers who work for the organization helped persuade the Supreme Court to reject a dangerous challenge to legal services for the poor, and it has prevented excessive secrecy in the court system. Its Mandatory Arbitration Abuse Prevention Project is a national leader in the battle against corporate efforts to use arbitration to eliminate court access. The honoree's litigation has exposed and stopped discrimination and unfair practices in the workplace on behalf of injured, low-wage women and minority workers.

Since 1982 Public Justice has fought for the rights of vulnerable consumers, earning its well-deserved reputation as the David against a Goliath who would close the courthouse doors on the disenfranchised.

Arthur Bryant, managing attorney, accepted the award on behalf of Public Justice. He began his speech by noting the involvement of Consumer Action and its employees in the precedent setting case, *Ting v. AT&T*, against binding mandatory arbitration clauses in consumer contracts. Darcy Ting, the lead plaintiff, is a former Consumer Action employee.

"We might have wanted to sue AT&T, but if we didn't have you

Continued on page 7

(L-R) Chris Heller, Jill Spickelmier and Mimi Barrett of Consumer Credit Counseling Services of San Francisco. (Nani Hansen photo)

Angelina Wong (L) and Rose Shirinian (R) of awardee KTSF Chinese News flank Consumer Action's Jamie Woo. (Ricardo Perez photo)

Arthur Bryant (L) of awardee Public Justice and Joe Orozco of Consumer Action. (Ricardo Perez photo)

(L-R) Cui Yan Xie, Angela Kwan, Kinny Li and Hazel Kong of Consumer Action greet party guests. (Ricardo Perez photo)

Audrey Perrott (L) and Yamin Chai of Consumer Action (Ricardo Perez photo)

Eric Batongbacal of AT&T (L) and John Gutierrez of Comcast. (Ricardo Perez photo)

Fariba Thomas of Union Bank (L) with Kathy Li of Consumer Action (Cui Yan Xie photo)

Continued from page 6

and Darcy Ting and consumers who are actually affected and are willing to join the case, we could not have made a difference at all," said Bryant, mentioning the role of longtime Consumer Action supporter, attorney Jim Sturdevant, in bringing the case. "It is Consumer Action and groups like you that really make sure that these victories happen and that they have the kind of impact they need to have to protect consumers."

Consumer Action activities

Our outreach and training team trained 796 representatives of community-based organizations (CBOs) at five regional meetings and 20 roundtables across the country. We distributed $175,500 in "mini-grants" to community-based organizations in seven states.

The DC office, working with fellow consumer groups, fought for the passage of federal legislation that would establish a consumer protection bureau with oversight of most consumer loans, limit the ability of huge corporations to harm our overall economy and to keep Wall Street in check.

Up next: 40 years

Join us on Facebook and Twitter as we approach our 40th anniversary in 2011.

On Facebook, we are facebook.com/consumeraction, and on Twitter we are twitter.com/consumeraction. ■

2010 Donors and Partners

Corporations & Businesses

Platinum Circle

Tracfone

Gold Circle

Capital One

Silver Circle

AT&T California | The Hastings Group | Humana | Microsoft | Union Bank | Vantagescore Solutions, LLC | Verizon

Benefactors

Copy Copies, Inc.

Sponsors

American Express | Consumer Attorneys Public Interest Foundation | Cuneo Gilbert & LaDuca LLP | Jack Gillis, Certified Automotive Parts Association | Southern California Gas Company | The Sturdevant Law Firm

Friends

Comcast | Consumer Federation of America | Credit.Com | CUNA Mutual Group | Nexus Communications | Rufus L. Cole & Associates

Individuals and Community Groups

Silver Circle

James S. Beck | Norman Bock | Neil Gendel

Benefactors

Jim Conran, Consumers First | Marsha Cohen | Pastor Herrera, Jr. | Patricia Sturdevant

Sponsors

Arnie Berghoff | Paul Bland, Public Justice | Trish Butler, Sage Communications | Consumer Credit Counseling Service of San Francisco | Linda F. Golodner | Dain Hansen | John Jensen

Friends

Chris Bjorklund | Stephen J. Brobeck | Chinese Newcomers Service Center | Consumer Federation of California (CFC) | Gregory Fowler | Ellis & Jennifer Gans | John Geesman, GreenEnergyWar.Com | Sue C. Hestor | Irene Leech | Erwang Mao | Martin Mattes, Nossaman LLP | Ralph E. Stone | United Policyholders

Educational Partners

American Express | Amplify Public Affairs | AT&T California | Brandeis University | California Consumer Protection Foundation | California Department of Insurance | Capital One | Consumer Federation of America (CFA) | Consumers for Auto Reliability & Safety (CARS) | The Hastings Group | Humana | JPMorgan Chase | Microsoft | National CAPACD | National Endowment for Financial Education (NEFE) | NeighborWorks America | The Rose Foundation | Sage Communications | Securities Investor Protection Corporation (SIPC) | Southeast Asia Resource Center (SEARAC) | TracFone Wireless | Verizon

Coalition Partners

Americans for Fairness in Lending (AFFIL) | Americans for Financial Reform | California Reinvestment Coalition (CRC) | Coalition for Patient Privacy | Consumer Federation of California (CFC) | Consumer Financial Protection Agency Coalition | Consumer-Labor Coalition | Credit Card Working Group | DC Advocates Coalition | Debt Relief Reform Working Group | Digital Due Process Coalition | EPIC Privacy Coalition | Fair Arbitration Now Coalition | Fake Check Working Group | Foreclosure Prevention Coalition | Fraud Alliance | Getting Older Adults Online (GOAL) | Health Care Reform Coalition (Families USA) | Identity Theft Prevention Coalition | Internet Privacy Working Group | Mortgage Coalition | Payday Loan Coalition | Small Dollar Loan Working Group | Subscriptions Upselling Working Group | Trans Atlantic Consumer Dialogue | Unemployed Homeowner Foreclosure Prevention Coalition

Cy Pres Awards

Consumer Action's work is supported in part with cy pres awards from these lawsuits:

In re ATI Tech. HDCP Litigation | Boehr v. American Express | Griego v. Rent-A-Center | Piscitelli v. Winn & Sims | Providian Credit Card Cases | Slayton v. Citibank | UCAN v. Bank of America | Van Etta v. Capital One Auto Finance | Ventura v. Providian National Bank | Wells v. Chevy Chase Bank

Many thanks to our educational network of more than 8,000 community-based organizations nationwide. We appreciate the work you do and respect your commitment to excellence.

Privacy lost: What's the harm?

By Linda Sherry

Often, when I mention to people that one of the areas we work on at Consumer Action is privacy, I get blank looks. It's a lot easier to understand why we monitor credit card rates or the insurance marketplace.

So then I find myself explaining why personal privacy is important. The first point I make is that once privacy is lost, it's essentially impossible to regain. Kind of like closing the barn door after your horse took off for the hills.

Common responses: "I'm not doing anything illegal, my life's an open book, I've got nothing to hide." Even so, you can be harmed by privacy violations—maybe more than you think. Would you want:

- Your credit card purchases to be public knowledge?
- People to track your location when you turn on your cell phone?
- Your insurance company to require that you install a "black box" in your car so it can monitor where you go, how fast you drive and how often you hit the brakes?
- Your ex to be able to track where you drive by monitoring your electronic toll pass?
- Your employer to know that you've had several miscarriages and you were receiving fertility treatment to become pregnant?
- Your coworkers to know that your daughter has a drug addiction problem?
- Your local newspaper to publish a photo of you coming out of the public pool with your breasts exposed because your bikini top fell off?

Okay, so you may not object to every one of these examples, but you probably get the point. Loss of personal privacy can have serious consequences.

Fortunately we do have some privacy rights, such as the right not to have our telephone conversations listened to. (On second thought, maybe Homeland Security never heard of this one.) All joking aside, your bank records are confidential, your first class mail is confidential, even your video rentals and records of the library books you borrow are confidential. All are protected against unreasonable search and scrutiny.

But most modern invasions of privacy involve new technology—new threats could be waiting just around the corner. Who would have envisioned all the ways that our privacy could be violated in 2010? Marketers track us as we surf the Internet. Full body X-rays and scrutiny by "behavior detection officers" are the price of getting on a plane. In some malls, facial recognition software helps digital signs display messages just for you. You can lose that job or that apartment by revealing too much on Facebook.

To put it simply, these are the reasons that we fight for privacy rights. There are real harms. Maybe these harms aren't as easy to conceptualize as exploding Ford Pintos, but we need to remain diligent against incursions into our personal privacy. We ought to choose if we want our lives to be open books! ■

'Like' privacy?

How to set your Facebook privacy preferences

This spring, Facebook unveiled new privacy settings for users. A new "user interface" makes it easier to keep information private and allows you to tighten the basic settings, which by default are not the most privacy protective.

If you'd like to protect information on your Facebook account with the highest privacy settings (which essentially means only allowing your friends and some advertisers to see it), take the following steps:

1. Go to Facebook.com. Under the "Account" tab on the top right hand side, click "Privacy settings."
2. Click "Friends Only."
3. Click "Apply These Settings"
4. Go to the tab called "Applications and Web sites."
5. Using their new drag and drop feature, across from the tab for "Games and Application Activity," select "Friends Only."
6. On the "Info accessible through your friends," select "Edit settings." Uncheck all the boxes and click "Save changes."
7. Go to the "Instant Personalization" tab. Select "Edit settings" and uncheck the box at the bottom of the page. Click "Confirm."
8. On the "Instant Personalization" page, select "Back to applications."
9. Under the "Public Search" option, select "Edit settings" and uncheck the box entitled "Enable public search." Click "Confirm."

If you'd prefer to keep more things public or semi-public, use the options above but select "Friends of Friends" or "Everyone" (which means the entire Internet will be able to see) under the various categories. ■

Facebook

Continued from page 1

to asking its users before it makes any changes to the site, such as sharing users' personal information with third parties or automatically enrolling them in new programs that result in users being forced to further link or share their personal information."

De Mooy cited "Instant Personalization" as an example of a new program released by Facebook. Instant personalization is a feature that can instantly share your Facebook information with the company's "partner sites" such as Yelp, the online ratings site. Facebook says its partners are carefully chosen and contractually required to respect Facebook users' privacy settings.

Guise of openness

De Mooy suggests that the company must recognize that consumers are increasingly aware of their privacy online and tired of companies giving away their information under the guise of openness.

"People care about privacy now more than ever," De Mooy said. "We are pleased that Facebook has pledged to improve user control and choice, and we look forward to working together to help them follow through on this commitment."

She suggests that the company must work with a broad coalition of consumer and privacy advocates, regulators, and legislators in order to raise the bar on online privacy principles, and lead the industry toward empowering and protecting consumers online.

De Mooy says that she hopes that advocacy by Consumer Action and other organizations will "send a message to industry that strong privacy standards aren't just good policy, they're good business."

Consumer Action believes there are still areas that need improvement on Facebook, such as empowering users with the ability to decide exactly which third party applications can access their data. Users can help protect themselves by changing their settings—either piece-by-piece or by category of information—to restrict sharing of their information.

Consumer Action has prepared a how-to guide on protecting your privacy using Facebook's new settings and controls. *(See the story in the box above.)*

You can ensure greater privacy when using social networking sites if you take a few simple steps:

Be a privacy advocate. For many social networking sites, much of your personal information is made public by default. This means the default privacy settings allow anyone to see and share your information, including your photos and list of friends. Take the time to read the company's privacy policy, check out the privacy settings page and place restrictions on any information you don't want the world to see.

Don't post key personal information. Finding out your date of birth (especially if it's combined with other information such as your city of birth), email address or even physical address, is a real gift for an identity thief. Any one of these, used in combination with publicly available information, can give crooks access to a host of personal information and financial accounts.

Keep your "on vacation" or "away" status to yourself. Unless you would post a sign on your front door that reads: "Now is a good time to rob me," don't provide "away" status updates. Thieves read social networking sites, too.

For more information on this and other privacy issues, please visit Consumer Action's educational website www.privacy-information.org and our main site www.consumer-action.org, and read our free privacy rights publications. ■