CONSUMER ACTION NEWS

www.consumer-action.org • February 2013

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

Mobile Privacy Issue

The privacy landscape

By Michelle De Mooy

Consumer privacy continues to be at the forefront of technology policy and proposed legislative action in Washington. All signs point to 2013 being as active as 2012, if not more so.

Last year began with the February release of the Obama Administration's Consumer Privacy Bill of Rights, which called for a multi-stakeholder process to develop voluntary industry codes of conduct around consumer privacy. The National Telecommunications and Information Agency convened the process.

Consumer Action hit the ground running as part of the stakeholder process, and has been at the forefront of crafting the codes. Consumer Action, the World Privacy Forum, the American Civil Liberties Union and the Application Developers Alliance collaborated to offer sample "short-form screens" for mobile devices that would provide consumers with information about who is collecting their personal data and for what purpose.

States have also stepped up to the plate to demand privacy protections for tech users. California Attorney General Kamala Harris signed an agreement with major app developers requiring them to display privacy policies in mobile apps before consumers initiate a download. California, Maryland, Michigan and Illinois also passed laws to prohibit employers from asking employees or prospective employees for their social media usernames and passwords.

The Federal Trade Commission (FTC) has not been idle on the issue of privacy. The agency investigated the data practices of several high-profile tech companies, including Google, Facebook and Spokeo, and it plans to conduct a study on data brokers this year as part of its plan to issue guidance for industry best practices.

In December, the FTC updated the Children's Online Privacy Protection Act (COPPA), which essentially prohibits behavioral advertising to children under 13. Among other improvements, the revised Rule now includes geolocation information as well as photos, videos and audio files that contain a child's image or voice in the definition of "personal information," and prevents third-party advertisers from secretly collecting children's personal information without parental consent. The agency indicated it would investigate indus-

See "Privacy landscape," page 4

A mobile primer

The who, what and why of data-ready devices

By Monica Steinisch

Buy airline tickets, shop for new shoes, send money to someone in another country, check your bank balance and deposit a check, post photos to your social networking page, check in at the airport, buy a cup of coffee, download software, play a game, make a donation, revise a document, apply for a job, watch TV, get directions, check the weather and find information about a health condition—there's not much of daily life that can't be carried out on a mobile device.

There's no question that mobile has caught on. According to the International Telecommunications Union, there were more than one billion

See "Mobile primer," page 3

Online, you are a 'digital goldmine' for marketers

'Do Not Track' advocates seek to limit online surveillance and establish consumer controls

By Linda Sherry

Each day, growing numbers of consumers go online via desktop computers, mobile devices such as a phone or tablet, video games and streaming video devices. But the vast majority of them are not aware of the personal scrutiny that goes along with modern-day technologies. Data—especially, but not limited to, information that helps businesses predict who you are and what you'll do and buy—is a "digital goldmine" used to build extensive profiles about your background and interests.

Software such as "cookies" and "beacons" can track users' browsing activity across the Web, collecting data. Just a click on a computer or other data-enabled device, such as a mobile phone or tablet, has the potential to collect information and connect the digital dots to build a profile that may include such attributes as your income range, shopping habits, current location, family size, education level and profession, just to name a few. Websites that provide free content make money by targeting ads to you, which they're able to do by using data they've obtained about you. Consumers, though they may not be aware they are doing it, voluntarily provide details about themselves in the course of accessing free services.

Despite the ongoing activism of privacy and consumer advocates, collecting user data is legal and consumers don't have much say in the matter. Regrettably, most data collection is done without your knowledge or permission by a vast ecosystem of companies, many of which are far from being household names.

Do Not Track

In 2007, the World Privacy Forum invited leading privacy and consumer groups to a meeting about online privacy. At that meeting, the Forum's director, Pam Dixon, proposed the idea of Do Not Track, a consumer protection tool based on the popular Do Not Call Registry, which required telemarketers to remove registered consumers from their calling lists. Similarly, Do Not Track would give consumers a "one-stop shop" to opt out of online (and offline) tracking.

The outcome was a collaborative proposal to the Federal Trade Commission (FTC) signed by nine organizations, including Consumer Action, urging the Commission to consider a federal Do Not Track Registry. The proposal would have required that online advertisers submit their information to the FTC, which would compile a machine-readable list of the domain names used by those companies to place cookies on users' machines and devices or otherwise track consumers. Following meetings with the FTC, the idea languished in favor of existing self-regulatory opt-out programs designed by industry with little or no oversight by the government.

Do Not Track has survived as a concept for online consumer privacy protection, though its execution has been refined and adapted to today's tech-

See "Digital goldmine" page 2

Consumer Action
www.consumer-action.org

Consumer Action has been a champion of underrepresented consumers nationwide since 1971. A non-profit 501(c)3 organization, Consumer Action focuses on financial education that empowers low- and moderate-income and limited-English-speaking consumers to financially prosper.

By providing financial education materials in multiple languages, a free national hotline and ongoing financial services research, Consumer Action helps consumers assert their rights in the marketplace and make financially savvy choices.

Advice and referral hotline

Submit consumer complaints about consumer problems to our hotline:

hotline@consumer-action.org

(415) 777-9635 or (213) 624-8327

Chinese, English and Spanish spoken

San Francisco

221 Main St., Suite 480
San Francisco, CA 94105
(415) 777-9648
Email: info@consumer-action.org

Ken McEldowney
Executive Director

Michael Heffer
Business Manager

Kathy Li
Director, San Francisco (S.F.) Office

Nani Susanti Hansen
Associate Director, S.F. Office

Audrey Perrott
Associate Director, Training/Outreach

Monica Steinisch
Senior Associate, Editorial

Jamie Woo
Community Outreach Manager

Joseph Ridout
Consumer Services Manager

Angela Kwan
Web Manager

Hazel Kong
Office Manager

Kinny Li, Cui Yan Xie, Tasneem Pitalwala
Project Associates

Ricardo Perez
Mail Room Operations

Rose Chan, Schelly Gartner, Vickie Tse
Consumer Advice Counselors

Alden Chan, Robert La, Andrew Taw
Support

Los Angeles

523 West Sixth St., Suite 722
Los Angeles, CA 90014
(213) 624-4631

Nelson Santiago, Linda Williams
Community Outreach Managers

Guo Guang Zhuo
Support

Washington, DC

P.O. Box 70037
Washington, DC 20024
(202) 544-3088

Linda Sherry
Director, National Priorities

(Editor, Consumer Action News)

Ruth Susswein
Deputy Director, National Priorities

Michelle de Mooy
Senior Associate, National Priorities

Alegra Howard
Associate, National Priorities

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

Consumer Action uses Bitly (bitly.com) to shorten lengthy Internet URLs in this publication

Privacy on a mobile device

By Michelle De Mooy

Personal data is the currency in today's hyper-tech economy. On the Web, data about individuals has become monetized into a robust engine of growth, fueling a wide variety of Web-based companies and services.

Much of this commercial activity is conducted out of sight of consumers—pulling back the curtain reveals a hive of business-to-business providers aiming to know you better so they can get your attention in a crowded marketplace.

This is particularly true for mobile devices, which are highly personalized, always on and always with us. Mobile has become a crucial platform for any industry because personal information about you, such as your sex and age, your purchase history or your browsing history, can be combined with real-time data such as your location so that advertisers are able to more effectively tailor and target their ads to you.

Mobile devices (cell phones, tablets and lightweight computers) are becoming, by far, the largest growing segment of the electronics market, spawning an entire advertising ecosystem revolving around personal data. Google alone had mobile advertising revenues of $2.5 billion in 2011. As more and more people own mobile devices, an astronomical amount of data is being collected and shared about individuals on a daily basis.

If personal data is the currency, mobile devices and apps are the financial pipeline. An estimated 50 billion apps were downloaded in 2012, and a huge majority of them were free. That's because developers and platforms (like Apple or Google) know consumers are used to free online content and don't like to pay for it. So they "trade" free services for information about you—even though you probably don't realize that you're making such a swap.

Even among consumers who willingly share information about themselves in exchange for free apps or targeted ads, studies indicate that many are concerned about this "data leakage" and desire greater privacy and more control over the data on their mobile device.

Mobile device users can batten down the hatches, but not all data leakage can be controlled without compromising the function of your device. (For example, if you turn off "location," you can't use map apps with as much ease, or use your browser to find nearby businesses.) The first line of defense is to visit the "Settings" area on your device, where you can make choices about privacy and security, such as establishing a screen lock and turning location services off and on. Under application settings, you can manage apps you've downloaded and check on running apps. If you can't find this setting, call or email your wireless service company to see if they can guide you. You could also use a search engine and type in "How do I change the privacy settings on a [your type of device]?"

If personal data is the currency, mobile devices and apps are the financial pipeline.

Apps are the biggest collectors and users of data. Many have default settings that enable them to access your device—even modify your settings—at will. More confusing, many mobile apps, such as Facebook or Twitter, have their own privacy settings. Read the app's privacy policy (if it has one) and consider visiting the company's website to get a tutorial on privacy settings.

Evaluate user reviews and other general information that may give you details about data collection and sharing before you download the app. If you suspect an app is not as described, or find its default requirements too intrusive, uninstall it and send an email to the company explaining your concerns.

It can be hard to figure out not only what personal information is being collected, but also who is doing the collecting. Different entities in the mobile device service chain collect different data and most have independent policies surrounding how long they keep and use it. Your phone's service provider, such as Verizon or AT&T, as well as the platform (Apple iOS or Google Android OS, for example) and your downloaded applications all collect information from your device. This might include photos, phone logs, calendar entries and contact information as well as text messages, financial information, gender and location.

All these "insights" into who you are and what you buy don't always work to your advantage. Researchers have discovered that "dynamic pricing," or prices that are variable depending on the consumer's profile and how many times they return to view an item, is widespread online and tends to disadvantage price-sensitive consumers from low- and moderate-income communities. For instance, coupons offered to wealthier consumers, ironically, tend to offer more money off than those targeted to low- and moderate-income consumers. A recent study from computer scientist Latanya Sweeney has also uncovered a possible racial bias in the ads Google serves to minorities.

Criminals haven't missed their mobile opportunity either, moving quickly to infiltrate devices through data-stealing malware or malicious apps.

Despite the real concerns about privacy in the mobile space, there are few laws and regulations in place to protect consumer privacy rights. *(See "A mobile primer," page 1.)* Consumer Action has worked hard to encourage lawmakers and policymakers to enact common sense regulations and laws that protect consumer privacy online. ■

Digital goldmine

Continued from page 1

nologies. Today's DNT is a browser feature (built-in or optional) or an optional application that tells websites you do not wish to be tracked. The proposal lived on in a 2010 statement by FTC Chairman Jon Leibowitz, and in legislative proposals in the 112th Congress and the California statehouse; in key privacy guidance documents created by the FTC and the Obama Administration; and in a global initiative by the World Wide Web Consortium (W3C). *(See "Privacy predictions," page 4.)*

The data industry says it does not buy and sell information that identifies individuals personally, such as names or email addresses, but that it aggregates anonymous data to build profiles of groups. Privacy advocates say this is little consolation, because anonymous data can easily be "re-identified," as demonstrated by New York Times and Wall Street Journal investigative reporters, among others.

FTC Chairman Leibowitz has said that, "Most consumers believe that a privacy policy protects their privacy. Instead, a privacy policy delineates their rights and their lack thereof." The policies have become more about protecting companies from liability than protecting consumers from invasive tracking and data collection.

Industry coalitions have developed voluntary tools for consumers to opt out of behavioral tracking across specific sites and ad networks, but these tools are not automatic and require ongoing vigilance from consumers.

Microsoft received heated criticism from its peers for adding Do Not Track (turned on by default in the installation flow) to a new version of its Internet Explorer browser. But, because publishers and advertisers are saying they will refuse to recognize the DNT signal, the impact may be lessened. Currently, no way exists for blocking data collection altogether.

What is collected?

Jeff Chester of the Center for Digital Democracy says the dramatic growth of the data broker industry, fueled by information on consumers culled from the Internet, social media, mobile phones and in-store shopping, has created "a multitude of all-seeing eyes spying on Americans everyday. A digital gold mine of infinite details is harvested about each of us—what we buy, who our friends are, how much we earn, our ethnicity, health concerns, location, etc."

Congress and the FTC are taking pains to learn more about what's collected on American consumers as they venture forth digitally. The Bipartisan Congressional Privacy Caucus, led by Reps. Ed Markey (D-MA) and Joe Barton (R-TX), last summer demanded that the nation's major data brokers provide extremely specific and detailed information about sources and methods for obtaining consumer information.

However, of the nine companies that received letters from the group of House members, only Acxiom agreed that it could be classified as a data broker. Epsilon, Equifax, Experian, Harte-Hanks, Intelius, Fair Isaac, Merkle and Meredith Corp. all said they should not be considered data brokers.

Recently, the FTC issued orders to nine data brokers to provide detailed reports on collection practices by Feb. 1, 2013. The companies are Acxiom, CoreLogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf

See "Digital goldmine," page 3

Mobile primer

Continued from page 1

mobile broadband (wireless Internet) subscriptions worldwide by the end of 2011. Half of all adults in the U.S. now own a smartphone, the most powerful type of cell phone, or a tablet, a compact computer bigger than a smartphone and typically smaller than a standard sheet of copy paper.

Despite their comparatively small size, these handheld computers can do many of the things a full-size computer can do, including stream videos, support multiple email accounts, and read and edit files. And they can sync with your desktop or laptop computer, meaning that you can share photos, files, contacts and other data across devices.

Mobile devices also allow you to do some things a standard full-size computer can't do, such as double as a baby monitor via an app or use GPS to pinpoint your location when you are looking for nearby restaurants.

Just like other computers, mobile devices run on an operating system (OS)—for example, Apple's iOS, Google's Android OS, or the Blackberry OS. The devices connect to the Internet via a data service plan (3G/4G) and/or Wi-Fi, which is a connection to the Web that can be secured (password protected) or unsecured (anyone can join).

Mobile devices are meeting the contemporary needs of an ever-moving, always-connected society as well as inviting a wider range of users than desktop or laptop computers do. Seniors have embraced tablets for a variety of reasons, including the ease of using a virtual keyboard on a screen that is touch-sensitive for arthritic hands. And the brightness and text size on a tablet can be adjusted, allowing someone with bad vision to read more easily. Not to mention, these devices make it easy to have "face to face" video phone conversations with family members and view the latest pictures of the grandkids.

And those grandkids are using tablets and mobile phones, too. According to Nielsen surveys, the majority of American teens (58%) age 13 to 17 said they owned a smartphone in July 2012, compared to only about a third (36%) of teens a year ago. For very young children, tablets and smartphones serve as distractors, babysitters, educators and toys. There are even apps available specifically for children under 2½ years old.

Because a mobile phone is much less expensive than a full-size computer—in many cases, it's free or heavily discounted with a service agreement—many low- and moderate-income households that could not afford to buy a traditional computer have been able to join the ranks of daily Internet users via a Web-enabled phone. A 2012 Pew Internet study found that about 40 percent of people in households earning less than $30,000 go online mostly through their phones, compared with just 17 percent of those earning more than $50,000. (Heavy data users, however, run the risk of exceeding the data allowance on their service plan and running up a larger monthly bill.)

Mobile offers many advantages, but there are numerous consumer protection issues that still need to be worked out. Front and center are the privacy risks that come with using mobile, including what goes on in the background, often without your knowledge or permission, while all those apps are doing their magic.

Caution warranted

These mini-computers that function as wallet, address book, mobile office, diary and more aren't always used with an eye to protecting personal information. Despite some progress in the right direction, lawmakers, regulatory agencies, advocates and industry still have not succeeded in implementing standardized, binding rules and codes of conduct to sufficiently protect consumers and their personal data.

As of now, the only federal protections for mobile users are those that apply to certain general categories of business (for example, the Financial Privacy Rule, which requires financial institutions to provide a privacy notice and allow consumers to opt out of having their information shared with certain third parties) and those that apply specifically to online privacy (for example, the Children's Online Privacy Protection Act (COPPA), which puts parents in control of what information a company operating online can collect about children under 13).

Since much of a mobile device's functionality comes from downloaded "apps"—software applications designed specifically for a mobile device—rather than the device's built-in browser, privacy-related rules for apps are crucial. But most mobile apps today don't even offer a privacy policy, in part because there's ambiguity about whether laws applying to online services apply to apps as well. In reality, users of many apps have no idea what kind of information is being collected through their phones and tablets, how it's being used, or what third parties it may be sold to for marketing or other purposes.

There are ongoing efforts on both the state and federal levels to hold app developers and others more accountable for how they collect, use and share consumer data. Until the law requires stronger safeguards from companies, it's up to you to protect your personal information. Experts agree that the single most effective way to avoid having your private information fall into the wrong hands is to use a passcode lock, which locks your device after a certain (short) period of inactivity. That way, if the device were ever lost or stolen, the data couldn't be accessed without the passcode.

It's also important to be selective about the websites you visit and the apps you download. *(See sidebar, "Apps and your privacy," for safety tips.)* Though a privacy policy, in and of itself, is not enough to make a website or app trustworthy, the lack of a privacy policy should be a red flag. When in doubt, look for a different website or app that can meet your needs—one that respects its visitors and users enough to offer both transparency and choice. ■

Apps and your privacy

What makes smartphones and tablets so powerful and versatile are the "apps"—special software applications that increase the device's functionality and make everything work better on a small screen.

There are apps that deliver newspaper content, allow you to play Scrabble and other games with your friends, tell you how your favorite sports teams did today, monitor the calories you've consumed, help you find a shelter in a natural disaster and do just about anything else you could imagine.

Even though a lot can be done via a mobile device's built-in Web browser, apps have the upper hand. There were 25 billion mobile app downloads in 2011, and that number was expected to reach 46 billion in 2012. Combined, the App Store and Google Play offer around 1.5 million apps.

Despite the steep growth in downloads, more and more consumers are becoming wary of apps and how much personal information they collect—and what they do with it. While websites have their own privacy issues—the use of "cookies," "flash cookies" and other technology to track Web surfers' online behavior, for example—statistics show that privacy issues related to apps are more troubling to consumers.

There are good reasons to be concerned about app privacy. While some apps depend on the ability to retrieve and share users' personal information stored on their devices (such as contacts, calendars, emails, texts and location) in order to function, many use this information purely for advertising purposes.

Generally speaking, apps can access most of the information in your phone without your direct consent, though some apps will ask for your permission to access more sensitive information such as your location.

While most users aren't willing to forgo apps completely, it's important to be selective. Here are some tips for safe app use:

- Only download apps from legitimate sources, such as Google Play (for Android) or the Apple App Store, to avoid exposing yourself to malicious code (malware) that could steal your private information. Apple has always done some minimal screening of the apps in its store, while Google recently introduced new rules for app developers that may help to reduce risks for its users.
- Vet your apps by first reading user reviews and making sure the developer is legitimate. If the app has a privacy policy, read it. Review and understand the permissions you are giving the app when you download it.
- Reject or uninstall an app if you're concerned about how much personal data is collected.
- Avoid apps that announce your location, which could compromise your personal safety or make your home more vulnerable to burglary.
- Review the privacy settings in the app itself, particularly in social media apps, to restrict who can view your personal content.
- Take advantage of parental controls to restrict your children's ability to download some or all apps.
- Once you've downloaded an app, don't just forget about it. First, if you have the option, set the controls or "Preferences" to limit what information the app collects and shares rather than simply accepting the default settings. (For social media apps, also customize the privacy settings in your social media account.) Then, for as long as you keep the app, install updates as they become available to ensure you have the safest version of the app on your device.
- Pay attention to notifications of a change in policy—apps and websites can change their privacy policies at any time, sometimes to provide less privacy. ■

— Monica Steinisch

Digital goldmine

Continued from page 2

and Recorded Future. The FTC asked for details about:

- the nature and sources of the consumer information the data brokers collect;
- how they use, maintain and disseminate the information; and
- the extent to which the data brokers allow consumers to access and correct their information or to opt out of having their personal information sold.

Competing on privacy

Many technology companies are beginning to understand that it can be good for business to build consumer trust online with robust privacy settings and controls. Privacy by Design (PbD), the philosophy of embedding privacy into technology by making it the default, has been embraced by many technologists, not only because it provides privacy controls to consumers, but because it gives companies a competitive advantage.

Browsers play a key role in allowing users to set privacy preferences and to block tracking software. However, when Microsoft announced last year that it would include the previously mentioned by-default Do Not Track mechanism in its new browser, the move was met with a backlash from online advertisers, who said they wouldn't honor IE 10's Do Not Track setting.

As consumers are becoming more knowledgeable about the need to protect their privacy, giving them adequate control is more crucial to business success. This is especially true among publicly traded companies, where a consumer data breach or greedy misstep in the handling of customer information could result in a public shaming that causes stock prices to drop. ■

Privacy predictions

Key players talk about 2013 privacy policy agenda

By Ruth Susswein

For the past decade, there's been a battle brewing about protecting consumers' privacy, both online and offline. Many predict that 2013, finally, may see some legislative and regulatory action on digital privacy.

Although an increasing number of consumers want stronger privacy controls, many of the companies that profit from the collection and use of personal information are digging in their heels to protect their "data goldmine" from new privacy regulations.

Consumer and privacy advocates—including Consumer Action—are fighting for individual control of personal information. The Obama Administration, Congress, the Federal Trade Commission and an international non-governmental body called the World Wide Web Consortium (W3C) all have proposals to safeguard digital privacy and protect consumers online. We've asked some of the nation's top privacy experts for their predictions: What will privacy look like in 2013?

Jules Polonetsky runs the Internet privacy think tank Future of Privacy Forum, which works with industry and privacy advocates to advance responsible online data practices.

JP: *In 2013, we will see mobile apps and mobile devices that use sensors to detect smell, heat, light and other information about individuals and their surroundings. We are already seeing apps showing up in smart cars and new smart home services. Increasingly, consumers are tracked across multiple screens and from online to offline stores.*

As more and more data is collected and used, it will be critical for companies to figure out how to provide consumers with effective and understandable options for how their data is used. And as important, companies will need to make the case to consumers of the value to users for how their data is used, or they will face a technical and regulatory backlash.

Senator Al Franken is a Democratic Senator from Minnesota. Last year, he introduced a bill that would require companies to get permission before collecting or sharing a person's location information from a mobile device. The bill passed the Judiciary committee at year's end, but did not become law. Senator Franken plans to reintroduce the Location Privacy Protection Act early in the new Congress.

AF: *Our federal laws allow companies to collect and share consumers' precise location information without their consent. These loopholes threaten the privacy of every single American who owns a smartphone, uses apps or owns an in-car navigation device. This is unacceptable, and that's why my location privacy bill will be a priority for this Congress.*

Chris Calabrese is legal counsel for the American Civil Liberties Union (ACLU). He's hoping that, among other consumer privacy protection improvements, we'll see an overhaul of the main statutory protection for the privacy of communications, the 1986 Electronic Communications Privacy Act (ECPA), including new rules that would require a warrant for government agencies to track anyone's location—by cell phone, smartphone or GPS. (Senator Patrick Leahy (D-VT), who chairs the Senate Judiciary Committee, announced that he expects his committee to tackle legislation related to email privacy and surveillance.)

CC: *Your inbox should have the same level of protection as your home. We need to update outdated electronic privacy laws so a warrant would be required for any private electronic information or communications—such as email, photos and cloud documents.*

ECPA was written before the Web was even invented. We are all increasingly living our lives online—learning, sharing, connecting and shopping—and we need laws that keep up with this modern online world. Since 1986, technology has advanced at breakneck speed while electronic privacy law remains at a standstill. Privacy law doesn't auto-update. It's time for Congress to modernize ECPA.

Pam Dixon is a privacy expert, head of the non-profit World Privacy Forum and creator of the Do Not Track (DNT) concept. She predicts that DNT will remain high on the privacy agenda in 2013 and that progress in defining DNT will advance with new leadership for the W3C.

PD: *My hope for DNT is that the parties involved in the W3C negotiations will find and move to a negotiated middle ground...I am hopeful that Peter Swire [the new chairman of the W3C] can move the needle on the discussions—he is skilled and fair. It's going to take movement from all parties and good faith.*

Frank Torres is Microsoft's senior policy counsel and director of consumer affairs. Last year, Microsoft included a DNT default setting in its Internet Explorer 10 browser, calling it "privacy by default," which means IE 10 browsers are not allowed to track you unless you change the setting to allow tracking. Microsoft says it's committed to giving consumers more control over their personal information online.

Torres expects DNT to continue to command a lot of attention in 2013, but he also predicts continued growth in "cloud computing" (online data storage on remote servers), particularly in areas such as healthcare and education. Torres says more transparency in how data is used and collected is needed.

FT: *[Microsoft] wants rules of the road to be clear in the cloud. As important as efficiency and cost savings are to cloud computing, we need to be mindful of the privacy and security aspects of those services.* ■

Privacy landscape

Continued from page 1

try players that don't honor COPPA.

Also in December, the FTC hosted public workshops exploring the privacy implications of online consumer data tracking/collection and online advertising practices.

Congress made little progress on passing a comprehensive privacy protection bill, but did take a few positive steps. An update to the Video Privacy Protection Act (VPPA) was passed that requires streaming video providers to obtain customers' consent in order to share information about their viewing preferences on social networks.

The video privacy legislation was weakened in January when the Senate tweaked the rules to allow blanket permission online (not to exceed two years or until consent is withdrawn by the consumer, whichever comes first) instead of requiring it on a case-by-case basis. Instead of the written permission called for in the 1988 VPPA, consent may be given via electronic means, online. (This bill was pushed by Netflix to allow its users to share their viewing history via social networks such as Facebook.)

Finally, the close of 2012 saw a last-minute push to clear Senator Al Franken's location privacy bill out of the Senate Judiciary Committee, which succeeded with some bipartisan support.

But the legislation, which would have required opt-in consent from consumers to allow location tracking on their mobile devices, never made it to the floor. Senator Franken has indicated that he will reintroduce the bill in the new Congress. ■

Privacy advice for digital transactions

While many security measures enhance the safety of digital transactions, online and mobile consumers may still face privacy risks. An open Wi-Fi connection, a lost smartphone or an accidentally revealed password could leave you at risk.

To help you make safe and secure transactions online and on the go, Consumer Action partnered with Visa Inc. to bring you free, impartial advice on how to protect your privacy. The "Digital Dollars" series of three brochures and a question-and-answer guide can be found on our website (bit.ly/digital_dollars). ■