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 privacy 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 industries 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

The 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

Mobile Privacy Issue

The privacy landscape

By Michelle De Many

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 Spotify, 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 industries 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 Spotify, 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 industries 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 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 industries 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 technology. 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 industries 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 technology. 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 industries 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 technology. 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 industries 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 technology. 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 industries 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 technology. 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 industries 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 technology.
Digital goldmine

Continued from page 1

logies. 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 was introduced in a 2010 statement by FTC Chairman Jon Leibowitz, and in legislative proposals in the 112th Congress. The California statehouse, in key legislation introduced by the FTC and the Obama Administration; and in a global industry 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. But in practice it can do so, 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 investigations (See “Privacy predictions,” page 4.)

The data broker industry, which relies on mobile opportunities 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 is concerned, but also who are lawmakers and policymakers to enact common sense regulations and laws that protect consumer privacy online. ■

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

It can be hard to figure out not only what personal information is being shared but also who is doing the collecting. Different entities in the mobile device service chain collect different data and most have industry standards for how long they keep and use it. Your phone's service provider, such as Verizon or AT&T, as well as the platform (Apple, Google, or Windows Phone 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 do, however, do not always work to your advantage. Researchers have discovered that "dyanmic 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. Data mining from computer scientist Latanya Sweeney has also uncovered a possible racial bias in the ads Google serve to minorities.

Consumers have 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. (See “A mobile primer,” page 1.) Consumer Action is concerned, but also who are lawmakers and policymakers to enact common sense regulations and laws that protect consumer privacy online.
Mobile primer
Continued from page 1

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 computer devices, mobile devices run on an operating system (OS)—for example, Apple’s iOS, Google’s Android OS, or the Blackberry OS. The device needs to be connected 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 the growth of things a desktop or laptop computer can do. Seniors have embraced tablets for a variety of reasons, including the ease of using a virtual keyboard on a screen that is easier to use for arthritic hands. And the brightness and text size on a tablet can be adjusted, allowing someone with bad vision to read more easily. Nor is mention of these devices made it easy to keep “face to face” video phone conversations with family members and view the latest pictures of your grandchildren.

And those grandparents 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 17 said they owned a smartphone in 2011. Half of all adults in the U.S. counts, 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.

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 allows financial institutions to provide a privacy notice and allow consumers to opt out of having their information shared with third parties) and those that apply specifically to online privacy (for example, the Children’s Online Privacy Protection Act (COPPA), which applies to websites and online services that collect information from children under 13).

Since much of a mobile device’s functionality comes from downloaded apps, the privacy considerations designed specifically for a mobile device—rather than the device’s built-in browser—privacy-related rules for apps are not as strong as rules for browsers. In reality, users of many apps have no idea what kind of information is being collected through their phones and tablets, and 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 accountable for 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. But, 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 app settings, and choose their new settings at any time, sometimes to provide less privacy. ■

Monica Steinisch

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 for almost every newspaper you might read, for playing 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 offered around 1.5 million apps.

Despite the steep growth in downloads, more and more consumers are becoming wise to 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 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 App Store, so you can avoid 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 security risks.

• Review 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 the app collects.

• Avoid apps that announce your location, which could compromise you or 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. But, 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 app settings.”

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 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 App Store, so you can avoid 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 security risks.

• Review 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 the app collects.

• Avoid apps that announce your location, which could compromise you or 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. But, 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 app settings, and choose their new settings at any time, sometimes to provide less privacy. ■

Monica Steinisch

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. ■
Privacy predictions

Key players talk about 2013 privacy policy agenda

By Ruth Suswein

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 in a warrant would be required for any personal electronic information or communications—such as email, photo or video stored via the Web. 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 stay up to date. It's time for Congress to modernize ECPA.

Pan 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 new middle ground. I am hoping that Peter Snow [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.

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.

FF: [Microsoft] wants rules of the road about 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 these 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 and 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 or opt-out 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 Consumer Action Help Center articles and answer guide can be found on our website (bit.ly/digital_dollars).