If you feel like somebody is always watching you, you may be right. Whether you are surfing the Internet, using a smartphone app to find the lowest gas price, streaming the latest movie to your laptop, tweeting about the presidential election, or using your iPad to put items in an electronic shopping cart, in all likelihood, someone is watching you.

Just about everything you do (where you go, what you buy, what catches your interest) is worth something to someone. And the more we use increasingly powerful computing ability and electronic connectivity, the more that businesses, employers, and total strangers are learning about us. Yet companies in the tracking business are increasingly finding that consumer groups, regulators, and media are watching them too.

Every day seems to bring another headline reporting tracking via search engines, smartphones, sniffing software, social media platforms, and the like. And with every new technological development that enables tracking, the question is posed whether new laws are needed to protect privacy. Yet, as we have seen with the “privacy” signs that we hang on hotel doors, the flip side of privacy is “service”—better information can lead to better service, which many of us find acceptable if we are aware of what is being collected and how it will be used.

With the pace at which the technology and the corresponding legal landscape are changing, in the United States and globally, it can be hard to keep track of all of the rules that govern e-tracking. On June 28th, 2011, the ABA Section of Science & Technology Law presented a dynamic panel discussion (free to SciTech members) that explored the emerging patterns in this new electronic reality, the corresponding legal standards, and practical ways to limit risk to reputation and the bottom line. It was my pleasure to moderate this panel, which included:

- Jessica Rich, Deputy Director, Bureau of Consumer Protection, US
What Is E-Tracking, and Where Does the FTC Stand?

The Federal Trade Commission’s (FTC) Jessica Rich started the discussion by outlining the agency’s position on e-tracking/behavioral advertising, which generally refers to the practice of collecting information online from consumers to serve them advertisements targeted to their interests. For well over a decade, the FTC has undertaken a number of initiatives related to e-tracking/behavioral advertising, including workshops and roundtables, reports and guidance, and cases it has brought under various privacy laws. The agency’s chief concerns regarding e-tracking are that it can, and often does, involve:

- collecting very sensitive personal information (e.g., about one’s health) across many websites and mobile devices,
- developing detailed profiles of consumers over time,
- sharing data with multiple parties, and
- using and sharing data further for other purposes.

Moreover, such practices occur invisibly and, until a few years ago, were largely unknown by consumers, who were offered very few choices.

After conducting a series of roundtables in 2009 and 2010, the FTC issued a preliminary privacy report in December 2010 that proposed that industry develop a do-not-track mechanism for online and mobile tracking. Rich emphasized that the agency’s recommended protection measures for businesses engaged in tracking go beyond the do-not-track mechanism, which has received a lot of attention, and are just one piece of the broader privacy puzzle that the agency is tackling.

The FTC Roundtables and the December 2010 Report

The FTC launched its project because of dramatic changes in recent years affecting consumer privacy, including the significant growth in mobile, social networking, behavioral advertising, and business models, as well as the increased collection, use, and sharing of data generally. The FTC launched the project to examine existing privacy frameworks and laws in the United States and abroad and to determine whether they were adequately addressing privacy in today’s world. Much of the roundtable discussions focused on the need for a new way of looking at privacy and a more privacy-protective framework. In particular:

1. Privacy by design, which means that companies should build privacy protection into their products and services at the outset, not later. Such built-in privacy protection should include:
   - Don’t collect more data than you need.
   - Don’t retain it longer than you need it.
   - Provide reasonable security for it.
   - Make sure it is reasonably accurate.

2. Meaningful consumer choice, which means making choice easier for consumers to exercise and also focusing consumers on choices that matter, while still allowing businesses to use data in ways that are consistent with and clear from the context of their interaction with consumers. No choices would be needed for certain commonly accepted practices, such as fulfilling an order, but meaningful choice would be needed for other practices. To be meaningful, the choice should occur outside the privacy policy, in a context when the company is interacting with consumers. Do-not-track is an essential piece of this framework and calls for an easy way to offer choice by providing a one-stop shop to allow consumers to opt out of third-party tracking.

3. Greater transparency overall, which means shorter standardized privacy policies that can be easily prepared, reasonable access to data (but the scope would vary depending on how data is used), and other protections.

The FTC’s Current Position on Do-Not-Track

Rich noted that the majority of the
FTC supports do-not-track as part of comprehensive privacy protection. The FTC has not yet proposed whether do-not-track should be implemented via regulation or self-regulation, but has been encouraged so far by industry developments. For example, Mozilla, Microsoft, and the Digital Advertising Alliance (DAA) have developed proposals to implement do-not-track in some form or another, and the FTC will be watching to see how these will develop.

Although the FTC has not specified particular technology for do-not-track, the agency has indicated that an effective mechanism would have five essential features:

1. **Universal**: it would apply as broadly as possible to tracking so consumers don’t opt out only to discover they are still being tracked in other ways.
2. **Persistent**: it needs to last over time and not be deleted when the consumer deletes cookies.
3. **Easy** for consumers to find, understand, and use.
4. **Effective and enforceable**.
5. **Must block not just advertising (for which the tracking is often used), but also the tracking itself**, except for certain data collection that is important for functionality (i.e., commonly accepted practices).

The FTC is pushing ahead to advocate for do-not-track and remains very concerned that e-tracking is invisible and that consumers need to receive more meaningful choices.

**Reactions to the FTC Position**
Jerry Cerasale indicated that the Direct Marketing Association (DMA) generally agrees from the 30,000-foot level with the FTC approach of telling consumers what is happening and giving them choices, but might disagree regarding the finer points of implementation. He indicated that the marketplace is there to provide the needed tools to provide the information the consumer wants, thereby increasing the efficacy of advertising.

Cerasale indicated that the DAA—a consortium of the nation’s largest media and marketing associations to which the DMA belongs—responded to the FTC’s Report by establishing the Self-Regulatory Program for Online Behavioral Advertising. This program promotes the use of the Advertising Option Icon (a blue triangle with a lowercase “i” inside, often called the “ad choices” icon), a symbol that generally is prominently placed on an electronic advertisement. By clicking on the icon, consumers can link to a disclosure statement regarding the participating company’s online behavioral advertising data collection and use practices, as well as to an easy-to-use, opt-out mechanism. The program uses a persistent cookie, is universal, and can go across browsers (it doesn’t matter which browser is used) and boundaries (e.g., it is now being pushed in Europe).

Consumers can go to www.aboutads.info to learn more about the program. Both the DMA and the Better Business Bureau (BBB) are participants and have self-regulatory enforcement programs in place. The program has already produced more than two trillion impressions (i.e., online ads displaying the icon).

Rich pointed out that the program only provides opt out for collection and use for behavioral advertising purposes, but companies could still collect and use data for other purposes. That is one area where the FTC is still debating with the DMA, DAA, and others. Although the FTC agrees that there must be some collection for fulfillment and basic functionality, the FTC believes that if a consumer opts out, data should not be used for any other nonfunctional purposes other than happy with what the FTC is doing, but consumer benefit versus harm can be a gray area. Most companies try to do the right thing and would like more guidance, but that can be hard to get without more enforcement action, which is not always the best way to set policy.

**Recent incidents show that efforts to anonymize data don’t always stick.**

**What Is Non-PII, and Is It Subject to Do-Not-Track?**
Rich noted that the terrain has changed regarding tracking of non-PII and more work needs to be done by technologists and industry leaders/experts. In line with the standard articulated in recent FTC reports, privacy protection should attach to data that can reasonably be associated with a specific person or specific device, because it is so easy now to put data together and take what is anonymous and reidentify it. If a business is using means to truly anonymize or aggregate data and feels comfortable that it cannot be easily reidentified by someone who might obtain it, the same protections would not need to apply. But some recent incidents show that efforts to anonymize data don’t always stick, including:

**Published in The SciTech Lawyer, Volume 8, Number 3, Winter 2012. © 2012 American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.**
• The 2006 AOL incident, where names were stripped out from user search queries that AOL released for use by academic researchers, but *The New York Times* was able to link the users with their search histories.

• The 2008 Netflix incident, where Netflix stripped out names and other identifying information from customers’ movie queues for use by researchers to improve algorithms for recommending films, but the researchers were able to use public information to identify specific Netflix customers and films they had rented.

Serwin stressed the PR issues associated with a data misstep. In conducting risk assessments, businesses should adopt a “data sensitivity approach,” where they look at the data elements themselves and consider whether they could be PII under any of the many definitions that are out there. He recently conducted a study with 125 data elements and two panels of consumers to get rankings regarding their beliefs about how sensitive various data elements were. Consumers were concerned whenever something happened to data, whether or not it was called anonymous.

Cerasale noted that the question of whether data is PII is a short-term question, because as individuals move increasingly toward smartphones and tablets (and away from a shared family computer and landline), the data on those devices becomes personal to that consumer.

**Enforcement**

Rich noted that the FTC is enforcing as aggressively as possible, using section 5 of the FTC Act for unfair and deceptive practices as well as various sectoral laws, including the FCRA (Fair Credit Reporting Act), GLB (Gramm-Leach-Bliley Act), CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act), Do-Not-Call (Telemarketing Sales Rule), and COPPA (Children’s Online Privacy Protection Act). Although the FTC is not enforcing the do-not-track mechanism under existing laws, the agency is pursuing many related cases, including:

• **In the Matter of Chitika, Inc. (2011),** where the FTC said that opt-out of targeted advertising from Chitika should last for a reasonable period of time, not just 10 days.

• **Google’s Buzz settlement,** where the FTC claimed that Google was deceptive in using information from G-mail users to create its social network contrary to what Google had promised. 5

• **Echometrics,** where the FTC said that the company sold software to enable parents to monitor kids’ online activities, but also sold that data to marketers.

On the litigation side, Serwin mentioned that both Apple and Google have been sued related to use of data by application developers. He mentioned the US Supreme Court’s recent ruling in *Sorrell v. IMS Health,* which invalidated an attempted restriction on a form of offline behavioral advertising on First Amendment grounds. 6 Increasingly, litigants are seeing an alphabet soup of claims, including under the CDA (Communications Decency Act), CFAA (Computer Fraud and Abuse Act), and the ECPA (Electronic Communications Privacy Act).

**Social Media and Behavioral Advertising**

Serwin indicated that the Lares Institute, a think-tank that focuses on emerging technology and information governance issues (for which he serves as executive director), released a report in June 2011 regarding social media usage patterns, the extent to which information is disclosed via social media, and the role of policies on social media platforms and within corporations. 7 According to the study, nearly 80 percent of people use social media, with nearly 100 percent of those under 18 using social media, while about 63 percent in the 66–75 age bracket are using it. Facebook has a particularly strong position: 94 percent of those using social media in this survey use Facebook.

According to this survey and other research Serwin conducted, consumers tend to read online privacy policies less than they read those made available offline. Consumers who are concerned about privacy (e.g., older generations, who are particularly concerned about health-related privacy) tend to read policies more. Consumers with higher education tend to read policies less. Privacy policies that are more interactive and easier to read might get consumers more engaged with the policy, but there is a need to balance this against the risk of deception. Social media use is going up, but only half of the respondents knew about their own company’s policy.

Cerasale indicated that the readability of policies would increase if marketers wrote them and lawyers then reviewed them to be sure nothing is wrong (companies frequently do it the other way around). He also emphasized that IT departments should not determine everything that a company does online and in social media; all too often, internal policymakers have no idea what is going on.

Rich echoed the concerns expressed as to whether privacy policies are working. The FTC recommends that disclosures be made in the context of the transaction: e.g., tell the consumer at the point of collection whether information may be shared with third parties, so that consumers are more likely to read the disclosures and make meaningful choices. She said that social networking is set up well to do that because people want to engage with the settings, which govern how information is used, instead of going off somewhere else to read a privacy policy. Unfortunately, the way social networks are set up now is cause for concern:

• Many practices are invisible despite the settings.

• They do not make clear that information is being shared with advertisers.

• There is no meaningful choice regarding the practices (except for sharing with friends). Other third-party sharing is not governed by settings.

• Kids and teens are using social
networking a lot, and they don’t have the same kind of judgment that adults do regarding tradeoffs in data collection.

- The appeal of interactive media is used as an incentive for collecting data, because more data can mean a more interactive experience/fun. Friend-to-friend marketing via social media is an example of this. (Cerasale indicated that the DMA has guidelines for such marketing, including checking to make sure friends have not indicated they do not want to hear from you, letting friends know why they are getting the communication, and giving the recipient the choice of no further contact.)

- The medium is moving increasingly to mobile, raising a host of unique privacy issues that will compound the social networking concerns.

Serwin indicated that many companies used to just collect a lot of information without worrying about what it was and were not disclosing a lot to consumers. Now, many companies are looking harder at their practices because they are concerned about regulations and the FTC (e.g., facing enforcement actions and getting biannual assessments for 20 years under section 5 of the FTC Act). Companies who really get it (and do a much better job on privacy) understand that this is a huge brand issue; they need to address the issue proactively and adopt best practices, or consumers will flee if they don’t do the right thing.

Cerasale concurred that targeted advertising, which is 64 percent more effective than untargeted advertising, is a brand issue; if it is not done right, people will flee. The marketplace and blogosphere are working by putting a bigger spotlight on what marketers are doing and making practices more transparent. Companies must become more transparent, because people will talk about practices they do not like, and the FTC is watching. Self-regulation needs to be given a chance to work. Regulation should only come in where there is market failure, and then should be as narrowly tailored as possible to address the particular issue. Otherwise, the economic consequences for the American economy could be long-lasting.

He added that when it comes to accessing and correcting data about one’s self, it makes a lot of sense if it concerns credit reports, and the law provides for that. But correction of information regarding inconsequential details (e.g., that the consumer bought a green sweater, not a red sweater) is not worth the time and money. Moreover, providing access actually can increase risk to the consumer by opening another door to potential breaches.

Mobile Data Collection

Mobile phones have so many unique features that they really raise the stakes, according to Rich. The phone is always on, is always with you, and is very personal to you, regardless of where you are and what you are doing. It collects location data, which is very sensitive, because it shows where the consumer is at all times. This is why the iPhone incident drew so much consternation. In addition, multiple parties can collect data directly or behind the scenes. The lack of good privacy models for mobile means that there often is far more data collection occurring than is needed to accomplish the purpose. For example, a traffic or weather service might need location data, but should not need call logs. In reports and its own lab, the FTC has seen data collection that is more extensive than is needed to provide the service. Problems in reading privacy policies are further compounded when viewing them on a small screen—any impatience the consumer might have on a website will be much worse when being forced to click through 100 screens on a mobile phone. The bottom line is that there are real privacy challenges in the mobile space right now and not enough efforts to address them.

Cerasale noted that in the iPhone incident, there was no harm because data was not used, but there was definitely widespread concern about a capability of which many consumers were unaware. Echoing Rich, he noted that because mobile providers must know where you are to get messages to you and to receive messages from you, data must be collected from you (and the consumer expects this, and permission is implied). Beyond such uses, people wouldn’t mind getting a coupon for coffee as they are walking by Starbucks, so long as they agreed to receive such communications. It opens up a huge new realm of advertising—reaching people where they are. If companies are collecting data for marketing or some other purpose, transparency is key—yet, it also presents challenges, because mobile phones have tiny screens.

Serwin indicated that when doing behavioral advertising, whether online or offline, companies need to ask whether they really need identifiable data when running analytics. If data were deidentified enough (which can be hard to do), it would not be easily identifiable if the database is lost or hacked.

Cerasale indicated that many have questions regarding marketing to cell phones. Contrary to urban myths circulating on the Internet, there is no public directory of cell phones, nor will direct marketers soon get a list of cell phones and be able to market to them. The Telephone Consumer Protection Act of 1991 (TCPA) prohibits automated dialing of cell phones without permission. DMA guidelines go further by specifying that companies cannot make unsolicited commercial calls to a cell phone without express permission. Marketers do not even have to check the national Do-Not-Call list, because marketers must have permission to call cell phones. Both the Federal Communications Commission/FCC (through a contractor) and the DMA have a listing of all exchanges that were provided for mobile use, plus a daily update of landlines that have been ported to mobile. One-eighth or more of households don’t have a landline now, and that number is growing. Because marketers are required to update these records daily, they cannot claim they did not know that the number they called was a cell phone. The DMA advises its members...
to make proper disclosures up front in forms used to collect phone numbers.

For those automated marketing calls to cell phones that do occur illegally, consumers can file complaints with the DMA, the FCC, and the FTC (file at www.ftc.gov, and click on the box in the right-hand corner titled “Consumer Compliant? Report it to the FTC”).

Next Big E-Tracking Trends
In identifying the next big e-tracking trends, the panelists identified three:

1. **Mobile explosion.** Rich mentioned that everything is going mobile, and more attention will need to be focused on implementing more meaningful protection there.

2. **Facial recognition.** Rich indicated that facial recognition (e.g., when you go in a store, they know who you are) is on the rise. Cerasale said that facial recognition is starting to be used online, via social media photos, and that HR and college admissions personnel are increasingly using social media to check on people.

3. **The Tab age.** Cerasale said that we are living in the Tab age, where tablets are everywhere and present different issues as a hybrid of other technology (e.g., bigger screen than a straight mobile phone). Ruth Bro added that the iPad has been a game-changer, with increasing adoption at the enterprise level; some companies are issuing tablets with or without a desktop computer as a more cost-effective alternative to a laptop. According to Cerasale, based on a Washington Post article, iPads are replacing Blackberries.

How Companies Can Minimize E-Tracking Risks
The four panelists identified their top three take-away tips for companies to minimize risks when engaging in e-tracking and otherwise avoid claims that the phone’s too smart, the media’s too social, and the advertising’s misbehaving. Below is their collective input:

1. **Know your data.** Really understand what data you are collecting and how you are using it. Cerasale recommended that whatever you have—whether in a company app, website, mobile space, or social media space—don’t let the IT department have control. Make sure your company conducts a total review of the policy so you know what you’re doing and what information you have. Servin recommended creating a data table. The first question he asks when creating a privacy policy or advising on a breach is: What data are you collecting? When there’s a breach, 95 percent of the time no one knows what data was at issue.

2. **Disclose, disclose, disclose.** Companies can eliminate a lot of problems if they adequately disclose their information practices and take the surprise out of what they’re doing.

3. **Do what you promise.** Companies often breathe a sigh of relief once they draft privacy policies/information collection statements, but then go back to their busy schedules without thinking again about promises that have been made.

4. **Don’t collect more data than you need.** The more data you collect and retain, the more legal liability you are going to have.

5. **Make privacy core to the company.** Companies that do a good job on privacy don’t have the lawyers or marketers running it. Instead, it’s core to the company. Establish an interdisciplinary team, including a privacy steering committee (especially if dealing with a lot of data); some companies often overlook this critical step. Companies that build privacy in from the start have less risk overall, because all of the stakeholders have signed on and understand the choices that have been made as well as the legal risks.

6. **Don’t save data for longer than you need it.** Check any defaults or legacy systems to make sure your company is not inadvertently collecting or using information not necessary for your business model. In the vast majority area of FTC data security cases (more than 30 to date), Rich observed that many problems would have gone away if companies had not kept data they did not need any more (legacy data being collected by legacy systems). Servin added that half of the data security cases/consent decrees concern paper and that companies can cut risks dramatically by making sure they have proper disposal methods for paper.

7. **Get involved with the self-regulatory initiatives.** Make sure that every contract you have with anyone that puts an ad on anything you control has to adhere to the self-regulatory rules.

8. **Keep track of developments** in the press (pay attention to media/PR fiascoes and consumer outcomes over certain practices), in legislation, in the courts, and in enforcement by regulators (e.g., there is a pattern in the way the FTC approaches these issues—look for these nuggets in the FTC’s guidance and case settlements). Companies should not just look at what the law says, but continually gain a sense of where the law is going. Even if a practice is not illegal, companies should never underestimate the risk of being tried in the court of public opinion. Corporate reputations are easily cracked but not easily mended.

Endnotes
1. The June 28, 2011 program was provided for free to SciTech members as one of two free member-benefit teleconferences for the 2010–2011 bar year.
5. See complaint, news release, order, and other related documents at www.ftc.gov/opa/2011/03/google.shtm.
7. See the report at www.ciresinstitute.com/in-the-news/study-on-social-media.