

The FTC's Privacy Program Grounding Principles, Recent Initiatives

Jessica Rich, Federal Trade Commission
NIST ITL Lecture Series on Usable Privacy
December 1, 2014

Good morning. I'm delighted to be here today to speak to you about the FTC's work on consumer privacy. Not surprisingly, I'll be addressing many of the same concepts discussed by my colleagues, but from the perspective of the lead U.S. enforcement agency in this area. First, I'll give some background on the FTC for those of you don't know our work. Then, I'll talk about how we approach privacy, and describe some of our recent initiatives.

I. Background on FTC's Jurisdiction and Authority

The FTC has broad jurisdiction under the FTC Act to address unfair and deceptive practices in the commercial marketplace. The basic rules are that companies cannot make deceptive claims about things that matter to consumers or cause substantial injury to consumers in ways that consumers cannot avoid and that do more harm than good. The FTC Act is flexible by design so it can address different practices as they emerge and evolve in the marketplace. Investment fraud, spyware, pyramid schemes, false advertising, mortgage fraud, debt relief – they're all subject to the FTC Act. Starting in the mid-1990s, with the emergence of the internet as a commercial medium, we began using this authority to address consumer privacy and data security issues. Since then, our privacy program has grown and grown, just as the many uses of consumer data, and the challenges to consumer privacy, have grown.

The Commission also enforces a number of sector-specific statutes. Notably, we enforce one of the first privacy laws in this country, the Fair Credit Reporting Act, which imposes privacy and accuracy requirements on companies that handle sensitive consumer report information. We also enforce the Gramm-Leach-Bliley Act, which imposes privacy and security requirements on financial institutions; the Children's Online Privacy Protection Act, which protects kids' privacy online and in the mobile environment; and laws against

online companies to simply post a privacy policy – very few had one! But today, we are dealing with many other challenges, including the fact that most companies now have privacy policies but use them to bury their privacy disclosures in fine print legalese that consumers don't read or understand.

Our current privacy program seeks to address today's many challenges. Today, data is collected from consumers wherever they go. Almost everyone carries a smartphone, uses social networks, and browses and shops through various devices. Consumers are tracked as they walk down the street, shop in stores, drive in their cars, fly in planes, and even as they monitor their health or exercise using health apps. Much of this data collection is invisible, happening without consumers' knowledge or consent. And many of the companies that access this data are invisible too – consumers have never dealt with them or even heard of them. We are in an era of invisible and ubiquitous data collection, and privacy policies just aren't up to the job.

So how are we addressing these challenges at the FTC? We're not reinventing the wheel and we don't have to. We're adapting the basic fair information practice principles

–

a company's fundamental business model and not overlooked or added later as an afterthought. They also are far more cost-efficient for companies.

Easy-to use-choice. Second, companies should offer consumers choices that they can actually exercise – for purposes of this event, I'll call it “usable” choice. This means choices that are prominent and focus on data practices consumers are likely to care about.

More specifically, it means that companies shouldn't bury choices in privacy policies. Instead, they should provide key information and choices at a relevant time and context, when consumers are providing their data or making other decisions about it. We call these “just-in-time” notices.

Greater Transparency. Third, and as an obvious corollary to providing choice, companies should provide greater transparency about how they collect, use, and share data. Specifically, companies should give consumers reasonable access to the data collected about them and move towards standardizing and streamlining privacy policies
an

Our central message about Big Data is that the basic privacy principles still apply. Indeed, they are more important than ever as data practices become more complex and potentially confusing to consumers. We see market pressures to move in this direction too. Consumers are increasingly demanding privacy, as shown by, not just surveys, but by actions they are taking in the marketplace – for example, using phony user names and privacy protective tools online, and objecting to certain data practices by certain large companies and yes, the government. We see stories about privacy every day in the press, and that presumably reflects readership interest and demand. Many companies are also upping their game in privacy – hiring privacy experts left and right (sometimes from my staff!) and offering and advertising new privacy tools and features.

But many companies still haven't gotten the message, which is why we are still sounding the privacy drumbeat, through both enforcement and policy initiatives.

On the policy front, we've held public workshops on various Big Data developments to discuss how to adapt the basic privacy principles to emerging business models. For example, in November 2013, we held a public workshop to discuss "the Internet of Things." Among other things

determine consumers' likely response to product and service offers, and (3) devices that consumers increasingly use to monitor their health and exercise, many of which aren't covered by HIPAA. Finally, on September 15th, we hosted a workshop entitled "Big Data: A Tool for Inclusion or Exclusion?" The workshop explored how the categorization of consumers in the Big Data era may both create and limit opportunities for them

Data. Interestingly, one of the best tools we have in this area is one of our oldest – the Fair Credit Reporting Act. Passed in the 1970s to address the treasure trove of data being collected, invisibly and without accountability, by the credit reporting industry, the FCRA governs the use of Big Data to make some of the most important decisions about consumers there are – whether to give them credit, jobs, or insurance.

Recently, for example, we announced settlements with two companies that advise retailers on whether to accept consumers' checks based on their financial history. Our complaints alleged that TeleCheck and Certegy failed to have appropriate procedures to maintain the accuracy of this data. The companies each paid a \$3.5 million penalty to settle the charges. We've also obtained settlements with substantial penalties against data brokers Spokeo, Instant Checkmate, InfoTrack, and Filiquarian for selling data to landlords without complying with the FCRA's accuracy and privacy requirements.

Another important case addressing Big Data is our first Internet of Things case – against home video monitoring company TRENDnet. In that case, we alleged that the company failed to provide reasonable security for IP cameras used for home security and baby monitoring, resulting in hackers being able to post private video feeds of people's bedrooms and children's rooms on the Internet. It's great that consumers can keep an eye on their homes from work or monitor their babies from a downstairs monitor, but not when criminals can watch too.

B. Mobile Technologies

A second area of focus for our privacy program is mobile technologies. In the past few years, this area has become one of the main priorities at the FTC, in privacy and

more generally. Clearly, the marketplace is moving to mobile, and consumer protections need to move with it. Mobile technologies also raise special challenges due to the always-with-you, always-on nature of mobile devices; the ability of these devices to track your location and connect to each other; and, of course, the small screen, or sometimes no screen, that makes disclosures to consumers ever more challenging.

On the policy front, we've issued several recent reports on mobile privacy and mobile payments. Our two reports on kids' app privacy showed that most of the apps surveyed collected personal information from kids' devices – including unique device ID, precise geo-location, and phone number – and shared it with third parties without telling parents. These findings fell short of all three of the basic principles we have emphasized – privacy-by-design, consumer choice, and transparency.

Our report on mobile privacy disclosures, *Building Trust through Transparency*, followed up on this problem. It recommended that the app platforms, app developers, and third parties collecting data through apps all take responsibility for providing transparency and choices in this marketplace, and provided specific recommendations for each. It's a great report, and we think it's helped spur improvements. However, there are still many challenges in this industry, and much work to be done.

On the enforcement front, we've challenged a range of violations occurring in the mobile space. For example, we recently announced a case against mobile messaging app Snapchat for misrepresenting – as its main selling point – that photo and video messages sent through the app would disappear. In fact, the messages remained accessible to recipients of the messages who simply connected their mobile devices to a computer. We

also took action against Goldenshores Technology, the maker of a popular flashlight app, for its privacy misstatements. We alleged that the app promised it would collect data from users' devices for certain internal housekeeping purposes, but failed to disclose that it transmitted the device's location and device ID to third parties, including ad networks.

Finally, we've brought a number of cases involving the security of mobile devices. For example, we took action against mobile device manufacturer HTC, alleging that it failed to secure the software it developed for smartphones and tablet computers. These failures left the devices vulnerable to malware, which could send text messages, record audio, and even install additional malware on the devices without the user's knowing or agreeing to it. We also challenged the data security practices of two mobile apps – Credit Karma and Fandango – alleging that the companies failed to use proper encryption techniques to transmit data, putting consumers' sensitive financial data at risk.

C. Safeguarding Sensitive Data

And that's a good transition to our third area of focus – safeguarding sensitive consumer data. By sensitive data, I mean kids', health, and financial data, as well as precise geolocation information.

Protecting sensitive data isn't really a new priority – it's a basic privacy concept that goes back to the early days in privacy and will be with us for years to come. But in today's marketplace, the stakes are even higher for sensitive data as it's captured all day long and then used and shared in ways consumers would never expect.

Our work to protect sensitive data includes over 50 enforcement actions against companies that failed to implement reasonable security protections – including such

companies as Microsoft, ChoicePoint, TJX, Lifelock, CVS, RiteAid, and Wyndham. Many of these cases involved, not just consumers' financial data, but health information, account IDs and passwords, and other sensitive data. Although we've brought these cases under several different laws that we enforce, they all follow a similar approach, which is to examine whether the company implemented *reasonable* protections for the data it collected and stored. In determining whether a company's data security practices are reasonable, we look at a number of factors, including the sensitivity and volume of the consumer information it holds; the size and complexity of the company's data operations; and the cost of available tools to improve security and reduce vulnerabilities.

It's clear that, even as the threats to data are increasing, many companies still haven't implemented basic security protections. We read about new data breaches in the news every day. And we see the same problems again and again in our investigations – failure to address well-known vulnerabilities revealed by prior breaches; collection and storage of sensitive data well beyond what's needed for business purposes; poor training and oversight of employees and service providers; and failure to test protocols before going live. In other words, no privacy (or security)-by-design.

Given the risks to consumer data and the serious consequences, data security enforcement remains a critical FTC priority. The Commission also unanimously supports new federal legislation to enhance our authority in this area. The legislation would give us additional enforcement tools, such as the ability to seek penalties for violations.

