Remarks of Commissioner Edith Ramirez
Privacy by Design Conference
Hong Kong
June 13, 2012

Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission

Last year, *Forbes* magazine branded privacy by design "the new corporate hotness."[1] Privacy by design continues to be the buzz concept of the day in the privacy world. And it is an important part of what the U.S. Federal Trade Commission and many other privacy authorities around the globe now advocate. Today, I would like to tell you what the FTC has done to deploy privacy by design: we are using it in our new privacy framework, our recent enforcement actions, and in the work we are doing in APEC to facilitate the cross-border movement of data in a way that respects consumer privacy.

I. The New FTC Privacy Framework

In March, the FTC released a final privacy report that clarifies and fine-tunes a framework we first proposed in December 2010.[2] The final FTC report espouses three core principles: privacy by design, simplified choice, and transparency. As laid out in the report, these three concepts incorporate the full set of fair information practice principles, updated for the 21st century. The FTC advocates these concepts as best practices for companies to adopt now on a voluntary or self-regulatory basis. We have also called on the U.S. Congress to enact comprehensive privacy legislation that draws on the ideas in the FTC's framework.

---

[1] Kashmir Hill, *Why 'Privacy By Design' Is The New Corporate Hotness*, FORBES (July 29, 2011), *available at* http://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness/.

[2] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

A. Privacy by Design

The hallmark of privacy by design is a deliberate and systematic approach to privacy and data security. The FTC framework uses the term privacy by design to include the following:

First and foremost, companies should embed privacy and security into their products and services from the outset. Second, companies should only collect the data they need for a specific business purpose and should safely dispose of it when that objective has been accomplished. Third, companies should employ reasonable security to protect consumer data.

Fourth, the FTC advocates an organizational or process component; we call on companies to maintain data management personnel, procedures, and controls to help ensure that substantive privacy by design principles are respected at all stages of the design and development of products and services. Companies should have personnel with responsibility for privacy. The company must also assess and mitigate privacy risks before a product launches and afterwards to address any privacy risks. The size of the program depends on the size of the company and the consumer data it uses.

But privacy by design cannot be reduced to hiring a chief privacy officer, mandating employees to watch a privacy training video or fill out a checklist, or inserting a privacy policy into an app. The notion that consumers deserve a meaningful choice about how their information is used is a mindset that must be instilled into a company's culture. It must be something that an engineer or website developer instinctively thinks about when writing code or developing a new product. Respecting privacy must be considered integral to the innovation process.

This vision of privacy by design is not new. But it has greater urgency as a result of the nearly constant collection and sharing of consumer data that changes in technology have made

possible. Let me give you a few real-world examples that show the promise of privacy by design if it were to be embraced systematically:

- Apple's Safari browser blocks third-party tracking cookies by default. This feature is automatically turned on, making it easier for consumers to prevent unwanted tracking of their activity across websites.

- A number of companies, such as Google, Twitter, and Mozilla, now offer SSL encryption by default in some of their online products and services.

- The Microsoft Xbox 360 gaming console, when used with Microsoft Kinect hardware, tracks gamers' body movements so that on-screen avatars can mimic those actions. Microsoft made the privacy-conscious decision that Kinect should not automatically send skeletal tracking and facial recognition data back to Microsoft. Instead, the data is deleted once the gaming session ends.

In these examples, privacy by design helps lift the burden of privacy protection off the shoulders of consumers. Too often, privacy protection depends on the notion that consumers can read and understand the legalese of lengthy privacy policies. The FTC's new framework seeks to steer away from that unrealistic vision of privacy protection.

B. Simplified Choice

That leads me to the second core principle in the FTC's framework: simplified choice. Companies should give consumers clear and simple choices about their data at a relevant time and context, outside of lengthy privacy policies or terms of service.

But under the FTC's framework, not all uses of consumer data require choice. To determine whether choice is necessary, the FTC framework looks to the context of the

interaction between the business and the consumer. If a data practice is not consistent with the context of the interaction, choice should be given.

In connection with online behavioral advertising, one way to simplify choice is through "Do Not Track," which is one of the FTC's most visible privacy initiatives. To the FTC, Do Not Track means a universal, one-stop tool for consumers to permanently opt-out of tracking across websites. We also believe that Do Not Track should go beyond opting consumers out of receiving targeted advertisements. It should stop the collection of data across websites for all purposes other than those that would be consistent with the context of the consumer's interaction with a website, such as capping the number of times a particular advertisement is shown and preventing fraud.

The FTC first called for Do Not Track in December 2010, at a time when the idea had little industry support. Our call for Do Not Track has since mobilized three key sets of players: the browsers, the U.S. online media and marketing industry, and the technical standards community.

Shortly after the FTC endorsed Do Not Track, Microsoft and Mozilla began to offer browser-based tools for consumers to communicate to websites their desire not to be tracked. Apple Safari and Opera later followed, and recently Yahoo! and Google have announced they will deploy Do Not Track mechanisms in their browsers later this year. Microsoft also recently announced that the next version of Internet Explorer will come with Do Not Track turned on by default.

Of course, a signal from a browser that a user does not want to be tracked is useless if it is ignored by the websites and marketers receiving the message. The U.S. online media and marketing industry, led by the Digital Advertising Alliance or "DAA," has launched an opt-out

program that uses icons in online ads. That program was designed to operate separately from browser-based tools, but in February the DAA committed to honor browser-based choices made by consumers. Major online presences like Twitter have also pledged to adhere to Do Not Track. Importantly, the DAA has also promised to ban its members from transferring online tracking data for use in determining employment, credit, insurance, and health care eligibility. That prohibition addresses a critical privacy concern a number of us at the FTC have expressed. In addition to these efforts, the World Wide Web Consortium or "W3C," an Internet standard setting body, is creating a global technical standard for Do Not Track.

Significant issues remain before the FTC's Do Not Track vision will been realized. But I am hopeful that we will have a viable Do Not Track system in place in the near future, and I look forward to industry's continued efforts to make that happen.

C. Transparency

The third principle in the FTC's framework is transparency. Companies should disclose details about their collection and use of consumer data. As I mentioned, the FTC urges companies to provide simplified choice to consumers beyond lengthy privacy policies. But the FTC does not want privacy policies, which provide a comprehensive, public description of a company's data practices, to be eliminated. We do, however, want to see privacy disclosures simplified and standardized so that consumers can compare data practices across companies.

II. Next Steps on the Policy Front

In the next year we expect to tackle several key recommendations in our report. For example, we recently held an FTC workshop addressing how to make effective privacy disclosures on mobile devices. We will update our industry guidance based on the information gathered.

We will also look at what we refer to as large platform providers, such as Internet Service Providers, operating systems, browsers, and social media. These companies have the potential to track nearly all of an individual's Internet activities. This raises serious privacy concerns that we will explore in a workshop later this year.

The FTC will also take part in the U.S. Department of Commerce's project to encourage the creation of privacy codes of conduct. Earlier this year, the Obama Administration issued a White Paper on privacy calling for businesses and privacy advocates to create privacy codes for specific sectors, such as the mobile industry, that would be enforced by the FTC. The Administration has also unveiled an online privacy bill of rights, which it urges Congress to enact and make enforceable by the FTC.

III. Enforcement: Facebook, Google, and Frostwire

The FTC has done extensive policy work in privacy, but we are at heart an enforcement agency. And we have recently resolved enforcement actions against two titans of the tech world, Facebook and Google, as well as a P2P app developer called Frostwire. In each of these matters, privacy by design figured prominently.

A. Facebook

The FTC's case against Facebook stems largely from a December 2009 overhaul of Facebook's privacy settings. Overnight, Facebook took information that was private—such as a user's "Friends List"—and made it public by default. Last November, the FTC charged that Facebook sprang these changes on its users without warning or permission and in violation of the company's privacy promises.[3]

[3] *See Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed complaint and consent order), *available at* http://ftc.gov/os/caselist/0923184/index.shtm.

We also charged Facebook with making misleading statements about the data shared with third-party apps on the site. Facebook told consumers that third-party apps could access only the user information that the apps needed to function. In fact, apps could see nearly all of the user's personal data. A TV quiz app, for example, could view a user's relationship status. We also alleged that Facebook made promises that it failed to keep. For example, it promised to delete the photos and videos of users who had deleted their accounts and then did not do so. Facebook settled the FTC's claims by agreeing to an order that broadly prohibits it from misleading consumers about how it protects consumer information. The order also prohibits Facebook from sharing consumer data with a broader audience than allowed by a user's privacy settings unless the user expressly consents. That means that before Facebook can relax its privacy settings, it has to ask its users first—and users have to say yes. If a user deletes data she posted or closes her account, Facebook must now take no more than 30 days to block others from getting access to her personal information, such as her photos and videos.

The order also compels Facebook to institute a broad privacy program that will apply to the site as it is now and to the design of new features and other changes. Facebook will have to designate personnel with responsibility for privacy. It must also conduct privacy risk assessments to ensure that it does not collect, use, or reveal information without its users' permission. The order also mandates outside privacy audits of Facebook every other year. Facebook will have to abide by the order for the next 20 years or risk daily fines of up to $16,000 per violation.

The upshot of the comprehensive privacy program and outside audits is that Facebook is now legally required to proactively take privacy into account. The order, in other words, mandates privacy by design.

B. Google

The FTC's action against Google involved Google's rollout in 2010 of its now-defunct Google Buzz social network.[4] Perhaps in its rush to launch a product to compete with Facebook, Google used Gmail accounts to populate the Buzz social network. In doing so, Google took the frequent contacts of Gmail users, which had been private, and made them public. We charged that this was done without users' consent and in violation of Google's privacy policy.

Significantly, the resulting settlement order applies to the full array of Google's many products and services. Under the order, Google cannot misrepresent how it treats consumer data. It also cannot change a product or service in a way that makes consumer information more widely available to third parties without getting consumers' affirmative express consent. As with *Facebook*, each order violation can result in civil penalties of up to $16,000 per day. Collectively, the FTC's orders against Facebook and Google will benefit well over a billion consumers across the globe.

C. Frostwire

I would also like to tell you about an FTC privacy enforcement action against a lesser-known company called Frostwire.

Frostwire designed mobile P2P software downloaded by hundreds of thousands of individuals on Android devices. Last October, the FTC charged that Frostwire's Android application caused its users to unknowingly share their pictures and other data.[5] Frostwire had set the default settings to automatically reveal private photos and videos taken with users' phones to other P2P users around the world. The Frostwire desktop app had never worked that way, and

[4] *See Google, Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (complaint and consent order), *available at* http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf.
[5] *See FTC v. Frostwire LLC*, No. 11-23643-CV (S.D. Fla. filed Oct. 11, 2011) (complaint and consent order), *available at* http://www.ftc.gov/os/caselist/1123041/111012frostwirestip.pdf.

we alleged that many Frostwire users would not have understood that the photos, videos, and other files on their phones would be automatically shared. We charged that Frostwire's configuration of the mobile app in this way was an unfair practice.

Had Frostwire practiced privacy by design, it would have built its mobile app to guard against the unwanted sharing of private photos and other personal files with an entire P2P network. As a result of the FTC's lawsuit, Frostwire must now do so. Under a settlement order entered by a court last fall, Frostwire cannot use default settings that automatically share the files users have created. In other words, the order helps ensure that going forward Frostwire will follow privacy by design.

IV. APEC and Cross-Border Data Transfers

I would now like to turn to cross-border privacy issues and the role that privacy by design can play in that arena. Consumer data can now be transferred around the globe in the blink of an eye. That reality demands data privacy regimes that are interoperable.

The APEC Cross-Border Privacy Rules System, with which some of you may be familiar, is an attempt to create a voluntary and interoperable system that provides meaningful safeguards for consumer data. Privacy authorities, businesses, and civil society groups in the APEC region negotiated detailed privacy rules—the APEC Cross-Border Privacy Rules or "CBPRs"—based on nine high-level privacy principles. Businesses that want to participate in the CBPRs will submit their privacy policies and practices for review and certification by third-party "accountability agents." Upon being certified for participation, businesses are subject to oversight by their accountability agent and enforcement by privacy authorities like the FTC. After many years in the making, the APEC Privacy Rules System was approved by the APEC

Ministers last November, and the system is set to launch this year. The United States applied to participate in the system just last month.

I have been personally involved in developing the system since joining the FTC two years ago, along with other FTC and U.S. Department of Commerce staff. The privacy and legal regimes in the vast APEC region vary widely. But despite those differences, APEC members have come together to develop a system that reflects a consensus on what constitutes sound cross-border data protection. This approach of agreeing on common rules to which individual companies can pledge their adherence and that are enforceable in all participating economies represents an important way to bridge differences across jurisdictions.

I highlight the APEC system because privacy by design underlies much of the system's framework. The CBPRs require companies to undergo a comprehensive review of their privacy and security practices. By signing onto the APEC Privacy Rules System, a company effectively agrees to abide by privacy by design.

V. Conclusion

Whether a company is transferring consumer data across town or across the globe, privacy by design is a vital part of effective privacy protection. But ingraining a culture of privacy is not something governments can impose by fiat. As regulators, we can advocate privacy by design as a best practice; we can mandate comprehensive privacy programs in our orders; and we can encourage privacy by design through voluntary international regimes. But it is ultimately up to businesses to ensure that privacy by design is more than a slogan. I am encouraged by the efforts of many organizations to incorporate privacy by design, and I am hopeful we will see this more and more.

Of course, I also recognize that not all companies will meaningfully embrace privacy by design. Many companies face intense pressure to maximize profits from the use of consumer data, and some believe that giving consumers choices about their data will limit that profit potential. In my view, that is a short-sighted approach that ignores the benefit of using privacy as a selling point. But it is a view that many hold, and one that privacy authorities cannot ignore. That is why we at the FTC remain committed to vigorous enforcement of existing privacy and data security laws. And it is why we have urged Congress to enact comprehensive privacy legislation to better address the privacy challenges of the digital age.

I would like to close by thanking Commissioner Allan Chiang and his office for organizing this conference and for inviting me to speak. As the FTC and our counterparts around the globe increasingly advocate privacy by design, it is critical that we have programs like this one to flesh out this important concept.

Thank you.