Keynote Address by Commissioner Edith Ramirez
Federal Trade Commission

Federal Communications Bar Association/Practicing Law Institute
29th Annual Institute on Telecommunications Policy & Regulation
Washington, D.C.
December 8, 2011

Privacy at the FTC: A Look Back At 2011

I want to thank the FCBA and PLI for inviting me back to speak at this conference. Last year, I addressed the FTC's recent policy work on the privacy front. I am especially glad to be here again because it allows me to take a step back to reflect on what has happened in consumer privacy in the past year, and to consider what the future may bring.[1]

Over the last year, privacy burst onto the headlines time and again. In the spring, we heard about massive data breaches at Epsilon, Sony, and Citigroup that collectively exposed the personal information of more than a hundred million people.[2] Around the same time, many people were alarmed to read that Apple and Android phones may have been transmitting their location without their knowledge or consent.[3] This summer, facial recognition technology was in the news as Facebook rolled out a feature to automatically identify the people whose faces appear in the 250 million photos uploaded to its site every day.[4] And just last week, it was reported that a company called Carrier IQ, whose software comes installed on a wide variety of smartphones, may have the ability to capture and transmit information about consumers' every keystroke.[5]

---

[1] These remarks are my own and may not represent the views of the Commission as a whole or any other Commissioner.

[2] *See, e.g.*, Stephen Grocer, *Sony, Citi, Lockheed: Big Data Breaches in History*

Naturally, these and other privacy headlines caught the attention of Congress, where privacy is seen as one of the few remaining bipartisan issues. And 2011 is coming to a close with a number of privacy and data security bills pending on the Hill.

Against this backdrop of public outcry and congressional concern, privacy remains at the top of the agenda of the Federal Trade Commission. We have had an extraordinarily busy year in privacy enforcement, and made a few headlines of our own.

Initial Privacy Report: A Recap

When I was here a year ago, FTC staff had just released a much-awaited initial report on privacy that proposed a new privacy framework.[6] The report's main objective was to give consumers more control over their information without depriving businesses of the ability to innovate. To accomplish that, the report made three key recommendations to Congress, in the event it legislates on privacy, and to assist industry in adopting best practices.

First, the report advocates the good data practices that we describe as "privacy by design" — the idea that companies should embed privacy into their products and services from the outset. Second, the report urges simplified notice and meaningful choice. Where possible, that means short, just-in-time alerts and options, outside of the legalese of long privacy policies. In the context of online behavioral advertising, this means Do Not Track — a universal mechanism through which consumers can easily choose to opt out of the tracking of their activities across the Web. Third, the report urges more transparency. Companies that collect consumer data should tell you what information they have about you and what they are doing with it.

The report received a lot of attention, especially our call for Do Not Track. But the FTC has not stopped there. Far from it: In the last year we have taken on three online titans — Facebook, Google, and Twitter — as well as a host of lesser known companies.

Facebook

Let me begin with the Facebook complaint and proposed settlement, which the FTC announced last week.[7] Our case largely stems from an overhaul of Facebook's privacy settings nearly two years ago to the day. Overnight, Facebook took information that was private and made it public by default. This surprised and outraged many consumers. We charged that Facebook sprang these changes on its users without warning or permission, and in violation of the company's privacy promises. And that, we alleged, was both a deceptive and unfair commercial practice that violated the FTC Act.

---

[6] *See* FTC STAFF, PRELIMINARY REPORT: PRIVACY IN AN ERA OF RAPID CHANGE (Dec. 1, 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[7] *See In the Matter of Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (complaint and proposed consent order), *available at* http://www.ftc.gov/opa/2011/11/privacysettlement.shtm.

But we did not see the December 2009 changes as an isolated lapse by Facebook. Rather, our complaint paints a picture of a company that played fast and loose with the privacy of its hundreds of millions of users. In a litany of incidents, Facebook's privacy practices flew in the face of its stated policies. For instance:

> Facebook told consumers that third-party apps could see only the user information that the apps needed to function. In fact, apps could access nearly all of the user's personal data. A TV quiz app, for example, could access the user's relationship status.
>
> Facebook also repeatedly promised that it would never give advertisers any names or other information about the people who receive or click on ads. However, for about a year and a half, when users clicked on an ad, their user ID was often revealed to the advertiser.
>
> In addition, Facebook told consumers that they could limit the sharing of their information to their friends when, actually, it was shared with the third-party apps installed by the friends of the user, exposing things like a user's relationship status, status updates, and where they had gone to school.
>
> Facebook also told consumers that their photos and videos would be inaccessible once they deactivated or terminated their accounts. This was not true.

Facebook chose to settle these and the other charges in our complaint. The FTC's proposed order — which is now open to public comment and then will be put to a final Commission vote — imposes a three-part injunction.

First, it broadly prohibits Facebook from misleading consumers about how it protects the privacy or security of consumer information. This includes whether and how consumers can control their data, whether the data is disclosed to others, and what information Facebook is collecting about them. It is worth noting infrt is woher1u f

The proposed 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 conduct privacy risk assessments to ensure that it does not collect, use, or reveal information without its users' permission. The proposed order also requires outside privacy audits of Facebook every other year. The upshot is that Facebook must now proactively take privacy into account in all aspects of its business.

The order, in other words, mandates privacy by design. That is especially appropriate for companies like Facebook, whose stock-in-trade is the collection and use of data about an astounding number of consumers. While FTC staff advocated privacy by design in its initial privacy report, by putting it in an order, the FTC has put legal teeth behind its recommendation. Facebook will have to abide by the order for the next 20 years or risk fines of up to $16,000 per violation, per day.

Our Facebook case stands for a few key propositions. The first is that all companies must live up to the promises they make about privacy. Facebook argued to us that it is different, that people come to Facebook precisely because they want to reveal information about themselves. But consumers should always be the ones to decide how their information is shared, even on a social network like Facebook, and regardless of whether a web-based service is free. Even Mark Zuckerberg is now publicly embracing the view that consumer control is paramount. In discussing the FTC action last week, he stated that on Facebook "everyone needs complete control over who they share with at all times," and he acknowledged that Facebook had made a "bunch of mistakes" on privacy issues, among them the December 2009 privacy changes.[8]

Our case against Facebook also leaves no doubt that companies cannot change the rules midstream about how they use a consumer's information unless the consumer overtly agrees to the change. It means that companies must ask for your permission before they change the way they share your data, and not merely beg for your forgiveness after the fact.

re

dismissed it as a slap on the wrist.[11] We have heard the criticism that the order merely requires Facebook to do what it already must do under the FTC Act — tell the truth and get affirmative express consent for material retroactive changes to privacy policies.[12] We have also been criticized for not imposing a fine.[13]

I do not pretend that the FTC's proposed order is a panacea for all of Facebook's privacy issues. For instance, it is tempting to say that the comprehensive privacy program and outside audits will take care of all of consumers' privacy concerns about Facebook. These provisions hold great promise, but the fact remains that they are recent and therefore untested innovations in FTC privacy orders.

At the same time, much of the criticism of the proposed order appears misdirected. The order does not impose a fine because Congress has not given the FTC the power to seek civil penalties for violations of Section 5 of the FTC Act,[14] the law that we alleged that Facebook violated. But now, under the proposed order, Facebook can be subject to fines for order violations.

There are also other limits on our legal authority. The FTC's main tool is the prohibition on deceptive and unfair commercial practices. Our agency has used this prohibition remarkably well in the privacy and data security arena, but it is not the equivalent of a baseline privacy law. The requirement of a comprehensive privacy program designed to reasonably address all manner of privacy risks should help fill this void. And I am personally committed to ensuring that this provision lives up to its full potential.

---

http://www.pcworld.com/businesscenter/article/245162/privacy_groups_generally_cheer_ftcs_facebook_settlement.html; David Kravets, *Privacy Groups Generally Cheer FTC's Facebook Settlement*, WIRED, Nov. 29, 2011, http://www.wired.com/threatlevel/2011/11/ftc-slaps-facebook-privacy/.

[10] *See, e.g.*, *Bono Mack Says FTC-Facebook Settlement Good for American Consumers*, Nov. 29, 2011, http://bono.house.gov/News/DocumentSingle.aspx?DocumentID=270525; *Markey, Barton Statement on Facebook Settlement with FTC*, Nov. 29, 2011, http://markey.house.gov/index.php?option=content&task=view&id=4618&Itemid=125; John Eggerton, *Rockefeller Praises Facebook Settlement, But Says Legislation Still Needed*, BROADCASTING & CABLE, Nov. 29, 2011, http://www.broadcastingcable.com/article/477233-Rockefeller_Praises_Facebook_Settlement_But_Says_Legislation_Still_Needed.php.

[11] *See, e.g.*, Ryan Tate, *Facebook Just Played the Government*, GAWKER, Nov. 29, 2011, http://gawker.com/5863493/facebook-just-played-the-government; Therese Poletti, *Facebook Gets Wrist Slapped by FTC*, MARKETWATCH, Nov. 29, 2011, http://www.marketwatch.com/story/facebook-gets-wrist-slapped-by-the-ftc-2011-11-29.

[12] *See, e.g.*, Therese Poletti, *Facebook Gets Wrist Slapped by FTC*, MARKETWATCH, Nov. 29, 2011, http://www.marketwatch.com/story/facebook-gets-wrist-slapped-by-the-ftc-2011-11-29.

[13] *See, e.g., id.*

[14] 15 U.S.C. § 45.

Google and Twitter

With the recent attention paid to the Facebook case, it is easy to overlook that in October the FTC also finalized a broad order against Google,[15] and one in March against Twitter.[16]

The FTC's action against Google involved the company's botched rollout of a social network — the now-defunct Google Buzz. Perhaps in its haste to launch a product to compete with Facebook, Google paid little heed to consumer privacy when it used Gmail accounts to populate the Buzz social network. The result was a public outcry and an FTC complaint and order that provided the foundation for the *Facebook* settlement. The *Google Buzz* order imposes requirements very similar to the ones I have just discussed with respect to Facebook. Significantly, it applies to *all* Google products and services. Google must abide by the order in connection with Google search, Gmail, Android, YouTube, Google+, etc.

We sued Twitter for data security lapses that allowed hackers to gain control of accounts — including those of President Obama and Fox News. Our order prohibits Twitter from misleading consumers about privacy and data security, and requires Twitter to institute a robust data security program with outside audits for 10 years.

across websites. This year, we have stopped two such companies, ScanScout[18] and Chitika,[19] from making false claims about the ability to opt-out of tracking and required that they provide user-friendly opt-outs from future tracking.

Outside the enforcement context, a majority of us at the Commission have continued to press industry to adopt Do Not Track.[20] We first called for Do Not Track a year ago, and earlier this year articulated five essential features of a Do Not Track system. First, the system must be universal, so consumers can go to just one place to opt-out. Second, Do Not Track is — as the name suggests — about online *tracking*. Any system must do more than merely prevent the delivery of tailored advertising. It must give people control over the collection of information of their activities across websites. The system must also be user friendly. And, the opt-out should be a lasting choice that does not need to be re-set each time consumers delete their cookies or update their browsers. Finally, the system must be effective and enforceable.[21]

No system has yet to meet all of these criteria, but there has been substantial progress over the last year. Microsoft, Mozilla, and Apple have all incorporated Do Not Track features in their browsers. Separately, a coalition of advertising trade associations has rolled out a program with icons in online ads from which people can opt out of targeted advertising of the coalition's members. More needs to be done, but I am pleased that industry is now focused on this issue.

Peer-to-peer file sharing is another area in which we have been active. In October, we sued a developer of P2P file sharing applications called Frostwire that flouted basic principles of privacy by design.[22] On its mobile app, Frostwire's default settings automatically revealed the photos, videos, and documents on users' smartphones and tablets. And changing the default was not easy. We charged that this configuration was likely to cause consumers to unwittingly disclose personal files to millions of other P2P users, which amounted to an unfair commercial practice. The consent decree bars Frostwire from using such default settings in the future.

---

[18] *See In the Matter of ScanScout, Inc.*, FTC File No. 102-3185 (Nov. 8, 2011) (complaint and proposed consent order), *available at* http://www.ftc.gov/os/caselist/1023185/index.shtm.

[19] *See In the Matter of Chitika, Inc.*, FTC File No. 102-3087 (Mar. 14, 2011) (complaint and consent order), *available at* http://www.ftc.gov/os/caselist/1023087/index.shtm.

[20] *See, e.g., Prepared Statement of the Federal Trade Commission on Internet Privacy*, Subcommittees on Commerce, Manufacturing, and Trade and Communications and Technology. Committee on Energy and Commerce, U.S. House of Representatives (Jul. 14, 2011), *available at* http://www.ftc.gov/os/testimony/110714internetprivacytestimony.pdf.

[21] *See Prepared Statement of the Federal Trade Commission on the State of Online Consumer Privacy*, Committee On Commerce, Science, and Transportation, U.S. Senate (Mar. 16, 2011), *available at* http://www.ftc.gov/os/testimony/110316consumerprivacysenate.pdf.

[22] *See FTC v. Frostwire LLC*, FTC File No. 112-3041 (Oct. 11, 2011) (complaint and stipulated final order), *available at* http://www.ftc.gov/os/caselist/1123041/index.shtm.

The FTC has also been hard at work to protect the privacy of children online. Congress has entrusted us with enforcing the Children's Online Privacy Protection Act, or "COPPA."[23] In September, the FTC proposed wide-ranging changes to our COPPA Rule to ensure it keeps up with recent changes in technology.[24] Under our proposal, websites and apps directed at children under 13 would have to get parental consent before tracking kids online for the purpose of delivering behaviorally targeted advertising. Our proposal would also make clear that geo-location information is subject to COPPA.

Finally, I want to tell you about a workshop the FTC is hosting today to explore the emerging privacy threats from facial recognition software. Some say the proliferation of this technology will mean that even the most obscure among us can no longer take our anonymity for gran foC is hoNe mw8.4 keenoseblic.r4yscurCine Priva562.681 Tm.0008 Tc0 Tw(245Tj12 0

But I also think there will be an increasing number of consumers demanding greater protection and control over their personal information, as they gain greater understanding about what takes place with data in the digital world.

For these reasons, I anticipate that privacy will remain an area of great interest to Congress. It may be unlikely that any of the numerous pending privacy bills will become law in this Congress. But with each new public outcry over an incursion into consumer privacy, there will be mounting pressure on lawmakers to do something, and eventually a Do Not Track mandate or a comprehensive privacy law may emerge.

Whatever Congress chooses to do, privacy will remain high on the FTC's agenda in 2012. You can expect that the Commission will continue to press companies to be more transparent and give consumers meaningful control over their personal information. In the coming months you will also see the final FTC staff privacy report. And I can guarantee that the FTC will continue its vigorous privacy enforcement docket in 2012.

Thank you.