Beyond Cookies: Privacy Lessons for Online Advertising

Jessica Rich, Director, Bureau of Consumer Protection

AdExchanger

But – and there's a "but" coming – targeted advertising raises consumer privacy concerns, plain and simple. For one thing, it is far from clear that consumers even know that they are being "tracked" when they visit internet sites. Some consumers still don't know what cookies are. But we are so beyond cookies at this point, and online tracking is only becoming more invisible as technology advances in the marketing world.

Companies are creating single, universal identifiers to track consumers across multiple devices and connect them offline, email, and digital interactions. We are no longer talking about a single connection between a consumer's computer and mobile device. Companies hope to follow consumers across *all* their connected devices, including smartphones, tablets, personal computers, connected TVs, and even smartwatches and other wearables. This enhanced tracking is often invisible to users.

In addition to tracking consumers across connected devices, companies are also

concerns are exacerbated when the tracking involves sensitive information about, for example, children, health, or a consumer's finances.

Adding to this complexity is that most companies that obtain consumer data are behind the scenes and never interact with consumers. These companies include hundreds of data brokers that collect and combine data from multiple sources and develop detailed profiles for sale to other companies. Privacy policies

brought hundreds of cases addressing a wide variety of privacy violations across many industries – for example, false claims about sharing data with third parties, failure to provide appropriate security for sensitive consumer data, use of invasive spyware or invisible tracking mechanisms, and unwanted spam and telemarketing. To maximize our effectiveness as a consumer protection agency, we also conduct studies, testify before Congress, host public events, and write reports about the consumer privacy and security implications of new and emerging technologies and business practices. Over the years, our workshops and reports have addressed such issues as data brokers,

companies.[1] Consumers are especially concerned about data collection in an era of ubiquitous mobile devices. A 2014 TRUSTe study found that 87% of consumers were concerned about the data collected through smart devices, and 88% wanted control over this practice.[2] These concerns are translating into consumer action. Another Pew study found that

and actions, but also significant backlash from users.[5] Similarly, we saw a decidedly negative reaction to the emotional research studies recently conducted by Facebook,[6] and SceneTap's use of facial recognition software in bars.[7] And virtually every time Facebook changes its privacy settings, it creates a huge uproar, and sometimes revisions, because consumers care about their privacy settings.[8]

In addition, there is the prospect of legal action, not just by the FTC, but also by the States, European regulators, and class action lawyers. For our part at the FTC, we've brought numerous actions against companies, large and small, for privacy and security failures that violate the law. For example, we recently took action against *Snapchat*[9] for allegedly deceiving consumers that messages sent through the app would "disappear forever" after the sender-designated time period expired. This was the apps' fundamental selling point, but the FTC's complaint describes several simple ways that recipients could save snaps indefinitely, such as by using third-party apps to log into Snapchat.

Our Snapchat case also alleged that the company's failure to secure its Find Friends feature resulted in a security breach that enabled attackers to compile a database

---

[5] *See, e.g.*, Alyssa Newcomb, *Google Hit with $7 Million Fine for Street View Privacy Breach*, ABC News (Mar. 13, 2013), *available at* http://abcnews.go.com/Technology/google-hit-million-fine-street-view-privacy-breach/story?id=18717950; David Streitfeld & Claire Cain Miller, *Google Hastens to Show its Concern for Privacy*, N.Y. Times (Mar. 13, 2013), *available at* http://www.nytimes.com/2013/03/14/technology/google-uses-on-privacy-after-street-view-settlement.html?pagewanted=all&_r=0; Clint Boulton, *Google Buzz Privacy Backlash Not Anticipated, Google Says*, eWeek (Feb. 17, 2010), *available at* http://www.eweek.com/c/a/Messaging-and-Collaboration/Google-Buzz-Privacy-Backlash-Not-Anticipated-Google-Says-212091/

[6] *See, e.g.*, Matt Pearce, *Facebook Tinkered with Users' Emotions in Experiment*, L.A. Times (June 29, 2014), *available at* http://www.latimes.com/nation/nationnow/la-na-nn-facebook-research-20140629-story.html

[7] James H. Burnett III, *Privacy a Worry as an App Scans the Bar Scene*, Boston Globe (Dec. 26, 2012), *available at* http://www.bostonglobe.com/metro/2012/12/26/scenetap-facial-detection-company-brings-controversial-nightclub-app-boston/VGcRCA1LSSQZ4aFq3Vq26H/story.html

[8] *See, e.g.*, Jessica Guynn, *Facebook Removes Controversial Line About Teens in Privacy Policy*, L.A. Times (Nov. 15, 2013), *available at* http://www.latimes.com/business/technology/la-fi-tn-facebook-teens-privacy-20131115,0,2668591.story#axzz2lOlXWooo

[9] Snapchat, Inc., No. 132 3078 (F.T.C. Dec. 23, 2014), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter

of 4.6 million usernames and phone numbers.[10] Even apart from the FTC's case, there was a public outcry about Snapchat. The company suffered loss of goodwill and reputational injury with its users.

We've brought many other cases involving allegedly false promises about consumer data. In our case against the maker of the popular Brightest Flashlight app, the FTC's complaint alleged that the company said it would collect certain information for internal housekeeping purposes but in fact sold it to third party ad networks.[11] Our complaint against ad company Scan Scout said that the company provided an opt-out for cookies but, in fact, still tracked consumers through flash cookies.[12] Ad company Epic Marketplace, we alleged, made promises to consumers about the limited nature of its tracking but, in fact, used "history sniffing" technology to track consumers across the web, including when they visited sensitive financial and health sites.[13] Our complaint against Aaron's Rent-To-Own chain found that the company used surreptitious software to track its rental computers and, in the process, captured highly personal photos and account data through the computers' webcam and key logging software.[14] We alleged that TRENDnet, the maker of in-home video cameras used to monitor sleeping babies and homes for safety, failed to secure the cameras' software and, as a result, hackers were

[10] Brian Fung, *A Snapchat security breach affects 4.6 million users. Did Snapchat drag its feet on a fix?*, Wash. Post. (Jan. 1, 2014), *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/01/a-snapchat-security-breach-affects-4-6-million-users-did-snapchat-drag-its-feet-on-a-fix/.

[11] *In the Matter of Goldenshores Technologies LLC & Erik M. Geidl*, No. C-4446 (F.T.C. Apr. 9, 2014), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3087/goldenshores-technologies-llc-erik-m-geidl-matter.

[12] *ScanScout, Inc.*, No. C-4344 (F.T.C. Dec. 21, 2011), *available at* http://www.ftc.gov/enforcement/cases-proceedings/102-3185/scanscout-inc-matter.

[13] *Epic Marketplace, Inc.*, No. C-4389 (F.T.C. Mar. 13, 2013), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3182/epic-marketplace-inc; *see also Chitika, Inc.*, No. C-4324 (F.T.C. June 17, 2011), *available at* http://www.ftc.gov/enforcement/cases-proceedings/1023087/chitika-inc-matter.

[14] *Aarons, Inc.*, No. C-4442 (F.T.C. Mar. 11, 2014), *availab*

able to capture and post online the live feed of 700 cameras.[15] And we alleged that social network Path deceived consumers by collecting personal data from their mobile device address books, contrary to promises made in its privacy policy.[16] These are just some examples of ways your data practices could go wrong – the things you *don't* want to do.

Fortunately, most companies in this industry are doing a good job of avoiding these no-no's. And on this positive side, we see that providing transparency and choices about privacy is increasingly a selling point for businesses. We see more and more ads touting the privacy features for products, and more and more tools being marketed that are designed to help consumers protect their privacy. One example comes from the nation's largest data broker, Acxiom. Acxiom launched a web-based tool, "About the Data," that allows consumers to view portions of their marketing profile by seeing certain categories of information, like personal characteristics, vehicles, household finances and credit, purchases, and interests.[17] While it still has a long way to go and is by no means a perfect tool, it's a step in the right direction.

The advertising industry also has made 9(no84Td [(al)-9(o8i9/l)Tj 0.509 0 Td [(W)9(hile iF.

companies engaged in personalized advertising and marketing; enforcement mechanisms that give the standards teeth; and limits on marketing based on sensitive data.

Some believe that these efforts are simply designed to stave off regulation or government oversight. And, yes, I am sure that's part of it. But companies also sign on to these codes because they believe that privacy is a selling point that resonates with their business clients and consumers.

Of course, to be successful, these efforts must reflect what is actually occurring in the marketplace today. They also need to ensure that there are not loopholes and workarounds that undermine the consumer protections they purport to provide. For example, the rules should apply to all tracking techniques, not just the ones in use at the time the programs were developed. Notably, as I mentioned, companies are employing more and more non-cookie technologies, like device fingerprinting, that are hidden from consumers and harder to control. More companies are taking data collected offline and using it online. Companies also are merging cross-device data to create single marketing profiles. The disclosures and choices provided to consumers should apply to all of these forms of tracking. Otherwise, the protections being offered are illusory, applying only to a small percentage of the practices that are actually occurring. This undermines industry credibility and, ultimately, consumer confidence. It also could deceive consumers who believe they are making choices about tracking, period.

Similarly, the programs can't include exceptions that swallow the rules. For example, if they purport to limit tracking based on sensitive data, they shouldn't play games about what "sensitive data" means, such as defining medical data to mean only

official medical records. The NAI code is stronger than DAA's in this regard. Finally, the choices offered by the programs must be easy to find and easy to use.

One of the greatest assets a business has is the trust of its customers. As consumers increasingly demand privacy, companies can leverage this demand as part of a broader business strategy. There are real benefits that companies can realize in competing on privacy and gaining consumers' trust.

II. Privacy Rules for the Road

So I've told you that privacy is important to your bottom line. But how can you harness consumers' demand for privacy in your business practices? The FTC has set forth three basic principles for addressing privacy in today's marketplace, which we encourage every company to implement as part of its business model.[19] They are:

Privacy by Design: Companies should build in privacy protections at every stage as they develop their products and services. These protections include reasonable data collection and retention limits, de-identification of data where feasible, and sound data security and disposal practices. Privacy protections are most effective when they are part of a company's fundamental business model and not overlooked or added later as an afterthought. They also are far more cost-efficient.

I would like to focus in particular on de-identification, an important concept for your industry as you know. As part of Privacy by Design, the first choice is always to

[19] FTC Report, *Protecting Consumers in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

for its false claims, and those claims were false because a third-party ad network – that was pulling data off the app contrary to those claims.

In our case against ad network Epic Marketplace, the company described in its privacy policy how it used cookies to collect data regarding consumers' visits to companies within its ad networks. It failed to mention that it was also using history sniffing to collect information on consumers' visits all cross the web, including to websites related to fertility, impotence, menopause, incontinence, disability, credit repair, and personal bankruptcy.[22] This kind of omission is deceptive and illegal under the FTC Act. You can't purport to provide a consumer with choices and then honor those choices only for a subset of your practices. Our case against ad company Scan Scout stands for the same principle.[23]

Second, and related to my first point, be careful about who you do business with. If you buy information from bad actors, sell or share it with them, you could find yourself embroiled in a law violation. For example, in the FTC's case against data broker LeapLab, we alleged that LeapLab bought the payday loan applications of financially strapped consumers – which included names, addresses, phone number, employer, as well as

III. Conclusion

In closing, I want to emphasize that the Commission's central goal is to offer consumers truthful information and meaningful choices as they navigate the marketplace. And we have learned that when companies explain the "value proposition" to consumers and give them such choices, many consumers choose to continue to engage, or to allow use of some of their data, rather than opting out altogether. Giving consumers choices about their data is essential to building the trust necessary for the marketplace to flourish. In the long run, hiding the ball will erode consumer confidence, which benefits no one.