Beyond Cookies: Privacy Lessons for Online Advertising

Jessica Rich, Director, Bureau of Consumer Protection
AdExchanger Industry Preview 2015
January 21, 2015

Thank you. I'm delighted to be here today. I think this is the first time the Federal Trade Commission has taken part in this event, and I hope it's the beginning of an ongoing exchange between the FTC and this community.

As I look around this room, I see a technological revolution at the intersection of marketing and consumer data. The "Mad Men" era of advertising – where marketers pay a magazine or TV station to rent their audience and then use the real estate to grab consumers' attention – is gone. Now timing and context are everything. Advertisers are looking to connect with the right consumers, at the right time, and in the right context. To do that, they rely on a high-tech, personalized experience – one that uses the collection, analysis, and storage of information about who consumers are, what they do, and where they go, to make predictions about them and their behavior.

Before I go further, I want to make something very clear: the FTC recognizes that targeted advertising benefits consumers. It can deliver ads that are relevant to consumers' particular interests and, increasingly, it can do so at the very moment that consumers would be interested in seeing such ads. Targeted advertising helps support a diverse range of online content and services that otherwise might not be available, or that consumers would otherwise have to pay for. This business model benefits consumers, and we have no interest in jeopardizing it.

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 their 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, companies are expanding their use of techniques such as device fingerprinting – which was originally developed to thwart illegal copying and fraud – to uniquely identify a broad range of internet-connected devices and build profiles about the people who use them. These profiles are often supplemented with data obtained from various third-party offline sources, making them even more detailed and personalized.

Even those consumers who know about tracking and want to avoid it can't do so effectively. For example, in the case of device fingerprinting, there are no simple means for users to prevent it – which, unfortunately, may be precisely why some companies have embraced this technology. Without adequate safeguards in place, consumer tracking data may fall into the wrong hands or be used for unanticipated purposes. These

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 – if you have the will and ability to find them – are impenetrable. And the data is used for numerous purposes, and in contexts well beyond the original collection: for marketing products and services; to decide what content the consumer sees when they do a search; to set prices for consumers; and to make decisions about consumers' eligibility for important benefits.

These are the many challenges that consumers, companies, and we at the FTC are dealing with today. For those of you who aren't familiar with our work, the FTC is the nation's consumer protection agency, and protecting consumer privacy has been one of our top priorities for two decades now. We enforce a variety of laws, but our main law – the FTC Act – prohibits unfair and deceptive practices in the commercial marketplace. This means companies can't make false or misleading claims about their products and services, or engage in practices where the harm to consumers outweighs the benefits to consumers and the competitive marketplace. That's legal mumbo jumbo, but the important point is that by law and practice, the FTC weighs market benefits and harms as part of its enforcement and policy work.

The FTC Act is flexible by design so it can address different practices as they emerge and evolve in the marketplace. And indeed, over the past 20 years, the FTC has

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, privacy notices, mobile security, and identity theft, among many other topics.

In addition, we distribute and make available on our website consumer education and business guidance on a wide range of subjects, including kids' online safety, preventing and repairing identity theft, and computer security. This work is designed to prevent harm before it occurs, and is an integral part of our mission.

I. The Business Case For Privacy

The focus on privacy has changed enormously in the past ten years. Increasingly, privacy has moved from a simple matter of legal compliance, best left to lawyers and IT professionals, to a C-suite issue – part of a broader bottom line strategy as consumer awareness and demand for privacy continues to grow.

Today, there is evidence of real consumer concern about privacy, and even consumer reluctance to engage fully in the marketplace as a result. For example, a recent Pew study found that 91% of adults surveyed "agree" or "strongly agree" that consumers have lost control over how personal information is collected and used by

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 86% of consumers have taken steps to remove or mask their digital footprints – steps ranging from clearing cookies to encrypting email, and from consumers avoiding use of their names to using virtual networks to mask their IP addresses.[3]

Surveys also show that younger consumers care about privacy, despite assertions to the contrary. Yet another Pew study found that children and teens actively engage with their privacy settings on social networks, often set their profiles to privacy-protective settings, and value the control that the settings provide.[4]

Other evidence of consumer concern comes from their reactions to privacy and security breaches when revealed by companies or the press. The recent and numerous high-profile breaches – at companies like Target, Michaels, Neiman Marcus, Home Depot, JP Morgan, and yes, the NSA – have prompted concern and even outrage among consumers and lawmakers alike. A few years ago, Google's collection of data through Street View, as well as its launch of the Buzz social network using consumers' email contacts to create the service without consent, resulted in not only regulatory inquiries

[1] Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era* (Nov. 12, 2014), *available at* http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.
[2] The TRUSTe Internet of Things Privacy Index, 2014 U.S. Edition, *available at* http://www.truste.com/us-internet-of-things-index-2014/.
[3] Pew Research Center, *Anonymity, Privacy, and Security Online* (Sept. 5, 2013), *available at* http://pewinternet.org/Reports/2013/Anonymity-online.aspx.
[4] Pew Research Center, *Teens, Social Media, and Privacy* (May 21, 2013), *available at* http://pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx.

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-focuses-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. C-4501 (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. Even apart from the FTC's case, there was a public outcry about Snapchat.[10] 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), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3256/aarons-inc-matter.

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 important strides in providing more choices for consumers. Members of groups like the Digital Advertising Alliance (DAA) and Network Advertising Initiative (NAI) have agreed to privacy codes of conduct to address public concerns about online tracking.[18] Both programs include standards for

---

[15] *TRENDnet, Inc.*, No. C-4426 (Jan. 16, 2014) , *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.
[16] *U.S. v. Path, Inc.*, Civ. No. C-13-0448 (N.D. Cal. Jan. 31, 2013), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3158/path-inc.
[17] *See generally* https://aboutthedata.com/.
[18] Digital Advertising Alliance, *DAA Self-Regulatory Principles, available at http://www.aboutads.info/principles* (last visited Jan. 20, 2015); Network Advertising Initiative, *NAI Code and Enforcement, at* http://www.networkadvertising.org/code-enforcement (last visited Jan. 20, 2015).

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 easy 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 into 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.

limit the data that you collect and retain, and dispose of it once you no longer need it. However, when companies do collect and retain consumer data, we encourage them to de-identify it wherever possible. Many of the beneficial uses of online targeting data can be accomplished using de-identified data.

But de-identification is far from perfect. There is always the possibility that ostensibly anonymized data can be re-identified. To address this issue, you should bolster sound technical strategies for de-identifying data with a strong commitment and effective polices not to re-identify it. This means that companies should publicly commit not to seek to re-identify the data and should, through contract, require the same of those with whom they share data.[20] If you are going to rely on the notion that your data is de-identified, you need to take all reasonable measures to ensure that it really is.

Increased Transparency: Companies should improve the ways that they communicate with consumers about how their data is collected and used. We have all read long privacy policies written in legalese that are too long to read and virtually incomprehensible. Privacy policies should be easy to read and understand. Also, we encourage companies not just to rely on privacy policies, but to separately provide key information and choices at the time that consumers are providing their data or making other decisions about it. We call these "just-in-time" notices.

"Usable" Choice: Companies should give consumers easy-to-exercise choices for those practices that would come as a surprise, given the context and the consumers' overall relationship with the company. As an easy example, when a consumer purchases

[20] *Id.* at 21-22.

a car from an auto dealer, the consumer would expect the dealer to collect and use his information to send a coupon for an oil change. A consumer might be surprised, however, if the dealer sold his data to a data broker that appended it to a larger profile sold to marketers.

Now, for many people in this room, there may be no relationship with the consumer at all. This means that you need to find a way to provide consumers with information and choices that they will actually see, whether through your own choice tool, the types of mechanisms offered by DAA and NAI, or through the consumer-facing partners you are working with. The critical point is that consumers need to be able to find and use this choice.

In addressing privacy at your company, there are some key pitfalls to avoid. **First**, make sure that any claims you make about how you collect, use, or share data are *truthful* and *complete*. Since all of your activities are intertwined with those of other companies, this means you need to work with those companies to ensure that their practices are consistent with your claims.

For example, in the *Brightest Flashlight* case, which I discussed earlier, the app claimed that it would only collect information from the device for certain internal housekeeping purposes, but actually shared the device's precise location and unique ID with ad networks.[21] Also, the company purported to give consumers choice about this sharing, but started transmitting the data to ad networks automatically, even before consumers had an opportunity to exercise that choice. The app was liable in this scenario

[21] *Supra* n.11.

for its false claims, and those claims were false because a third party – the ad network – 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, or 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 Social Security and bank account numbers – and then sold this sensitive information to marketers whom it knew had no legitimate need for it.[24] These included: marketers that made unsolicited sales offers to consumers via email, text message, or

[22] *Supra* n.13.
[23] *Supra* n.12 (alleging that the company offered an opt out using HTTP cookies but still collected data through flash cookies).
[24] *FTC v. Sitesearch Corp. d/b/a LeapLab*, (D. Ariz. Dec. 23, 2014), *available at* http://www.ftc.gov/enforcement/cases-proceedings/142-3192/ftc-v-sitesearch-corporation-doing-business-leaplab.

telephone call; data brokers that aggregated and then resold consumer information; and phony internet merchants that used the information to withdraw millions of dollars from consumers' accounts without their authorization. We charged that LeapLab's sale of this data to scam artists and others with no legitimate need for it is an unfair practice under the FTC Act. This case is currently in litigation.

Similarly, in our case against home security company Versatile Marketing Solutions, we alleged that the company violated the FTC's Do Not Call rules by calling millions of consumers on the Do Not Call Registry.[25] VMS had purchased the consumer leads from companies that generated the leads illegally, and then ignored complaints from consumers who said they were on the Do Not Call list. A key message here is that you need to do due diligence about the consumer data you obtain from others.

Third, as I mentioned earlier, to be meaningful and non-deceptive, the information and choices you provide consumers must cover all of your tracking practices, not just a subset.

Finally, be very careful about marketing using sensitive data – consider avoiding it altogether but, at the very least, provide opt in. I suspect that even the cynics among you – who say that that despite all the hub-bub about privacy, consumers keep giving away their data – recognize the dangers of marketing based on such issues as cancer, aids, sexual preference, pregnancy, and of course marketing to kids.

[25] *U.S. v. Versatile Marketing Solutions, Inc., also d/b/a VMS Alarms, et al., and Jasjit Gotra*, Case No. 1:14-cv-10612 (D.C. Mass. Mar. 10, 2014), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3162/versatile-marketing-solutions-inc-also-dba-vms-alarms-et-al.

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 this marketplace to flourish. In the long run, hiding the ball will erode consumer confidence, which benefits no one.