Protecting Consumer Privacy in the Digital Age:
Reaffirming the Role of Consumer Control

Keynote Address of FTC Chairwoman Edith Ramirez
Technology Policy Institute Aspen Forum
Aspen, Colorado
August 22, 2016

Good afternoon, everyone. I am pleased to be back in Aspen to participate in this week's forum. When I was here three years ago, I highlighted the privacy challenges that big data presents and discussed the ways the Federal Trade Commission is working to safeguard consumer privacy in this time of rapid technological innovation.

A lot has happened in three years. At the time I spoke here in 2013, the word "selfie" did not appear in the Oxford English Dictionary, the Apple Watch was not on the market, and the mass production of self-driving cars was still seen as a distant goal.

The last three years have also given rise to new challenges in privacy. We have seen an explosion of surveillance technologies, such as drones and mobile device tracking sensors in retail stores. We have moved from an ecosystem where companies track consumers across websites to one where companies track us across apps and even across devices. And now, many consumer devices and appliances – from your fitbit to your fridge to your thermostat – are silently talking to one another, collecting data, and transmitting that information to various third parties. Even the once private act of reading is generating data about us, as e-book companies track not just what we read, but also *how* we read – where we start, what passages we skim, re-read, or highlight, and whether we actually finish the books we begin.

But even with these developments, the overarching challenge – fostering technological innovation and growth while protecting consumers' privacy – is a familiar one. Like the

gymnasts we watched perform on the balance beam at the Olympics in Rio last week, we must aim to strike the right balance – one that promotes innovation *and* protects privacy.

As new technologies and business models continue to emerge, however, we hear with increasing frequency the claim that technological innovation and big data have rendered certain fundamental tenets of privacy, particularly the idea of consumer consent, outdated and ill-suited for today's digital world. Rather than focus on consent, these big data advocates argue, we should apply use-based approaches that set specified limits on businesses' ability to use the data they have collected but allow everything else.

I disagree. I believe that the principles of transparency and choice that undergird privacy laws around the world – as well as the approach the FTC advocates – continue to play an important role in protecting consumer privacy. In order to build and sustain trust in the marketplace, consumers should be in the driver's seat when it comes to their personal information. If consumers feel that they have little or no control, there is a risk that they may not embrace the new products and services that companies seek to offer. We already see some evidence that many consumers are opting out of receiving ads altogether, as surveys show that the number of consumers installing ad blockers is growing.

There is no question that there are challenges, but I believe that companies are capable of developing innovative and creative solutions that can not only give consumers more control over their personal information, but also enhance privacy and promote productivity and growth.

I. Marketplace Changes Affecting Consumer Control

Before I turn more specifically to what companies can do, let me elaborate on the challenges. With the rise of big data analytics, the proliferation of connected devices, and the

emergence of other new technologies, we have seen the marketplace evolve in ways that have significant implications for consumer control.

First, it was not all that long ago that there was an inclination to think of privacy as an "all or nothing" proposition. Data was seen as either personally identifiable or not, and privacy protections were designed around clearly-defined categories of "personally-identifiable information." Consumer consent was often seen as either opting into, or out of, all data collection – with no middle ground. Today's landscape is much more complex.

Since the Commission released its first report on online behavioral advertising in 2009, we have discussed the increasingly blurred line between PII and non-PII.[1] As consumers use more digital devices and the sophistication of big data analytics increases, it has become significantly easier to identify individuals based on information not traditionally categorized as personal information, making it more difficult to protect their privacy. For example, in a study published last year, researchers examined purportedly anonymized credit card transaction records. They found that, with just four random pieces of information that could be gleaned from social media and other public records – such as the stores a person shopped at or movies the person rented – they could re-associate 90 percent of people with their credit card transaction history.[2] As a result of the increased ability to identify consumers, we now regard data as personally identifiable when it can be *reasonably linked* to a particular person, computer, or

[1] FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (Feb. 2009), *available at* https://www.ftc.gov/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral.

[2] *See* Natasha Singer, *With a Few Bits of Data, Researchers Identify "Anonymous" People*, THE NEW YORK TIMES (Jan. 29, 2015), http://bits.blogs.nytimes.com/2015/01/29/with-a-few-bits-of-data-researchers-identify-anonymous-people/; *see also* Yves-Alexandre de Montjoye et al., *Unique in the shopping mall: On the reidentifiability of credit card metadata*, SCIENCE (Jan. 2015), http://science.sciencemag.org/content/347/6221/536.full.

device. In many cases, persistent identifiers, such as device identifiers, MAC addresses, static IP addresses, and retail loyalty card numbers meet this test.[3]

Just as the distinction between PII and non-PII is not black and white, nor are consumer preferences. We know that many companies, including Google, Yahoo, and Acxiom, offer tools where consumers do not have to opt out of advertising completely, but can choose on which subjects they would like to receive advertising. These companies have noted that, instead of opting out fully, the majority of consumers who use these tools engage with them in a more nuanced way[4] – perhaps choosing to receive traveling and hiking ads, but rejecting other types of ads.

As these examples show, as an increasingly wide spectrum of data, with different levels of consumer preferences and expectations attached to it, gives rise to potential privacy concerns, privacy can no longer be thought of in terms of stark dichotomies.

Second, even putting aside practical difficulties like the absence of consumer interfaces for many devices, the sheer number of actors in the digital arena makes it increasingly difficult for consumers to make informed choices and understand where their data is going. In a world of connected devices, consumers often do not know which companies are doing what. On a mobile device, if I have a problem, should I turn to my carrier, my operating system, my device manufacturer, or my app? On a smart TV, I may be getting content from my cable provider, or a

---

[3] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (March 2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; Comment of the Staff of the Bureau of Consumer Protection to the Fed. Commc'n Comm'n (May 27, 2016), https://www.ftc.gov/policy/policy-actions/advocacy-filings/2016/05/comment-staff-bureau-consumer-protection-federal.

[4] *See, e.g.*, Comment #00417 from Google, Inc. to Fed Trade Comm'n 4 (Feb. 18, 2011) (Re Preliminary Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"), *available at* https://www.ftc.gov/sites/default/files/documents/public_comments/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework/00417-58065.pdf.

streaming video provider such as Amazon or Roku. At the same time, my TV manufacturer and TV apps may also be collecting my information.

Of course, companies that interact directly with consumers are just the tip of the iceberg. As we have discussed in our reports on the data broker industry[5] and big data,[6] dozens of companies operate behind the scenes, scooping up our data and using it to provide further insights about us, often in ways that consumers have little or no idea about. In addition to the data broker industry, the modern-day advertising ecosystem includes a number of companies – not only ad networks, but real-time bidding exchanges, supply and demand side platforms, data aggregators, measurement and analytics companies, and a host of others collecting our data behind-the-scenes. How is a consumer supposed to know about these companies, let alone make informed choices about them? And does this complex ecosystem allow companies to pass the buck to avoid accountability for privacy and security failings?

Third, the increase in the use of big data analytics to gain deeper insights about consumers and predict their preferences has the potential to weaken the effectiveness of consumer choice. As we have seen time and time again, big data is "big" because of the scale and variety of information that companies can accumulate. But its significance is also magnified because of the sophistication of the analyses that can be applied to seemingly benign bits of information to make inferences about individuals, [7] often sensitive inferences, and draw

---

[5] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (May 2014), *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[6] FED. TRADE COMM'N, BIG DATA A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES (January 2016) [hereinafter *Big Data Report*], *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

[7] *See* PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, REPORT TO THE PRESIDENT BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE, at 19 (May 2014), *available at* https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

conclusions about their lives. These conclusions can have significant consequences for consumers, particularly when the data is used to determine eligibility for things like insurance, housing, and employment.

All of these developments raise difficult questions. Given that companies can use big data analytics to infer information about consumers without their knowledge or consent, how can we ensure the effectiveness of consumer choices? Given the multiplicity of actors involved, how can consumers possibly understand where their information is going and what it is going to be used for?

While it may be tempting to conclude, as some do, that the idea of consumer control as a central privacy tenet is outdated and should be abandoned, I believe that consumer control remains paramount.

Now, some might argue that this view flies in the face of reality – consumers cannot possibly make informed choices in this complicated era of big data, companies cannot provide disclosures on devices with no screens, and by relying on consumers to make their own decisions, we are going to cut off valuable sources of data that will have beneficial uses for society.

I recognize the challenges. But I think that building consumer trust is essential if we hope to unleash the full potential of big data, and that enabling consumers to control the collection, sharing, and use of their information is key to establishing that trust.

Let me be clear that I am not saying that consumer control is everything. Existing privacy protections rightly reflect a number of use-based restrictions, among them the Fair Credit Reporting Act which the FTC enforces. I also agree that we have to continue the conversation about acceptable and unacceptable uses of consumer data. And, as the FTC has emphasized in

our report on big data earlier this year, companies need to be mindful of the limitations of big data analytics and the potential for adverse consequences for consumers, especially low-income and under-served communities.[8] But, in my view, consumer control is essential to protecting privacy, and technology can be used to help us achieve it.

II. Role of Industry

So what can industry do? I see a distinct role for three types of companies: companies that offer products and services directly to consumers; companies that operate behind the scenes, such as data brokers and ad networks; and what I will refer to as "privacy intermediaries."

First, companies that offer products and services directly to consumers should be transparent about their data practices and should improve consumers' ability to manage and express their privacy preferences. As the Commission noted last year in our report on the Internet of Things, companies can offer innovative ways to allow consumers to communicate these preferences. These include set-up wizards and settings menus through which consumers can make initial choices, as well as dashboards where consumers can revisit and modify their choices. Many social media websites and apps, smartphone platforms, and IoT devices already offer this capability. This type of innovation is promising, and I hope to see more of it in the future.

Second, behind-the-scenes entities should also offer and respect consumer choices. Providing choices poses an additional challenge for these entities because consumers may not know who they are. For ad networks, this problem can be addressed by respecting consumer choices expressed through platform or browser tools. By way of example, as of February 2016,

[8] *See Big Data Report*, *supra* note 6.

nearly 17% of consumers used the limit ad tracking setting on their iOS and Android devices.[9] Additionally, surveys suggest that 30 to 50% of Internet users delete their cookies every month.[10] Ad networks should refrain from using techniques that circumvent these types of consumer choices.

As for data brokers, the FTC has called on these companies to develop a centralized Internet portal to identify themselves to consumers, describe their information collection and use practices, and provide links to access tools and opt outs. This approach would enable consumers to visit a single site to find out what kinds of information data brokers have about them and how to exercise opt-out choices.

Finally, I think there is a role for intermediaries to facilitate communication of privacy preferences between consumers and businesses. In other contexts, like the so-called "sharing" economy, we have seen the value that intermediaries can add to facilitate transactions between buyers and sellers.[11] The range of tools offered by privacy intermediaries might be as simple as privacy comparison charts or guides, akin to a Consumer Reports for privacy. For an Internet-connected TV or car, the tool could describe what categories of data are collected, whether data is shared with third parties, what the uses are, how long the data is retained, and how long the product or device is patched. I understand that some organizations are already exploring these types of tools.

---

[9] Kate Kaye, *Use of Limit Ad Tracking Drops as Ad Blocking Grows*, ADVERTISINGAGE, May 9, 2016, http://adage.com/article/privacy-and-regulation/limit-ad-tracking-drops-ad-blocking-grows/303911/.

[10] *See* comScore, The Impact of Cookie Deletion on Site-Server and Ad-Server Metrics in Australia, 14 (January 2011) (discussing various findings on consumer cookie deletion), *available at* https://www.comscore.com/Insights/Press-Releases/2011/2/comScore-Publishes-White-Paper-on-the-Impact-of-Cookie-Deletion-on-Website-Audience-Measurement-in-Australia.

[11] *See generally* FED. TRADE COMM'N, The "Sharing" Economy: Issues Facing Platforms, Participants, and Regulators, https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators.

Privacy intermediaries might also enable consumers to share their information only with businesses who meet certain criteria set by consumers. This type of tool could include feedback loops and rating systems, which would add an accountability component. Imagine a privacy app that allows me to create an account, specify what information I would like to share, and have companies compete for my business.

These intermediaries could also offer tools that allow consumers not only to express privacy preferences, but also to manage them. For example, a team of researchers at Carnegie Mellon are developing what they call a "personal privacy assistant."[12] This technology would allow your smartphone to automatically scan WiFi and Bluetooth channels for privacy policies that are being broadcast by other devices and then would either make determinations on your behalf or prompt you to make a decision. It would be capable of learning the privacy preferences of users over time and autonomously configuring many settings. So you would not have to worry about whether the terms of service for any of your devices have changed – your personal privacy assistant would do it for you.

Another technical tool for managing privacy preferences is "data tagging." Under this approach, consumer preferences could attach to and travel with data. This could be particularly useful as data is passed from consumer-facing entities to data brokers, ad companies, and others.

This is the type of innovation that I want to encourage to help give effect to consumer choices.

[12] *See* Lorrie Faith Cranor, *Personal Privacy Assistants in the Age of the Internet of Things*, World Economic Forum Annual Meeting 2016 (Mar. 15, 2016), http://opentranscripts.org/transcript/personal-privacy-assistants-internet-things/. For more information about the project, see: http://www.privacyassistant.org/index/.

III. Role of the Federal Trade Commission

The FTC also has an important role to play in empowering consumers and ensuring they have control over their personal information. We can do this by: (1) conducting research to ensure that our policymaking efforts appropriately address privacy and security risks as the marketplace evolves; (2) using our law enforcement authority to ensure that consumers' choices are honored and that companies safeguard the consumer data they collect; and (3) helping spur innovation in the creation of tools that help consumers express choices.

First, we will continue our research and policymaking efforts to make sure that our recommendations keep pace with innovation. In our reports on IoT and data brokers, we have discussed how the principles we set forth in our 2012 Privacy Report – privacy by design, improved transparency, and simplified choice – continue to apply in today's world of IoT and big data.

It is important, though, that we continue to re-evaluate and test our principles against new technologies and business models. This is one of the reasons we regularly host workshops and have placed a priority on research. In the coming months, as part of our Fall Technology Series, we will be looking at new challenges associated with the growth of ransomware, drones, and smart entertainment systems.[13] We are also examining how multiple companies delivering services on a single connected device interact with one another. For instance, we are collaborating with the Federal Communications Commission to study security updates on mobile

[13] *See* Press Release, FED. TRADE COMM'N, FTC to Host Fall Seminar Series on Emerging Consumer Technology Issues (Mar. 31, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-host-fall-seminar-series-emerging-consumer-technology-issues.

devices.[14] We are obtaining information from the operating systems and device manufacturers, while the FCC is asking questions of the carriers. Together, we hope to get a better picture of where the backlogs are in providing security updates and patches.

Next year and the year after that, there will be new challenges. The FTC will continue to study the issues, solicit input from stakeholders, and calibrate our approach as the marketplace evolves.

Second, as a law enforcement agency, we are committed to using our authority to make sure companies are protecting consumer privacy and safeguarding consumer data. A key part of that effort is ensuring that companies honor consumer choices. One recent case, against the operator of a large mobile ad network, InMobi, illustrates the need for continued enforcement in this area. InMobi offered app developers software code to embed in their apps to enable them to serve targeted advertising, including advertising based on geolocation. It represented that its software would track consumers' locations only when consumers had granted access to that information. The FTC alleged that, in actuality, InMobi had used consumers' geolocation information, which it was able to infer, to target ads, even when consumers had not granted geolocation permission. Among other things, we alleged that inMobi's actions were deceptive and therefore violated Section 5 of the FTC Act.[15] This case highlights that companies – even those that do not directly interact with consumers – ignore preferences set by consumers at their peril.

---

[14] *See* Press Release, FED. TRADE COMM'N, FTC To Study Mobile Device Industry's Security Update Practices (May 9, 2016), https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices.

[15] *See* Press Release, FED. TRADE COMM'N, Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission (June 22, 2016), https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked.

While protecting consumer choices on the front end, we also seek to ensure that these choices are not undermined on the back end, as they are when companies' lax data security practices create a risk that consumers' data will fall into the hands of wrongdoers. Our recent case against wireless router manufacturer ASUS highlights the importance of pre-launch security testing of IoT devices. There, we alleged that the company's failure to test its Internet-connected routers prior to launch contributed to several security breaches. We charged that ASUS' actions were both deceptive and unfair, in violation of Section 5.[16] As the risks of data breaches continue to increase, we will continue to use our enforcement authority to ensure that companies take reasonable steps to safeguard consumer data.

Finally, the FTC can also play a role in fostering innovation and incentivizing companies to develop the new privacy tools that I have discussed. We have done this before in the telemarketing arena. Recognizing that technological developments were making it more difficult to combat unlawful robocalls, we have sought to spur innovative technological solutions to this persistent problem. To date, we have conducted four public contests, offering cash prizes to inventors who propose technological solutions to the robocall problem. One of the winning solutions to our first robocall challenge, Nomorobo, was made available to consumers, and it now reports having blocked over 127 million robocalls.[17] We are developing similar types of challenges in the privacy arena.

Another way we can help incentivize innovation and research in the areas of privacy and security is to showcase the work of researchers. As an example, our workshop on disclosures next month will allow researchers to describe mechanisms to test the effectiveness of privacy

[16] *See* Press Release, FED. TRADE COMM'N, ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk (Feb. 23, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.
[17] *See* https://www.nomorobo.com/.

disclosures, which are critical to providing consumers the opportunity to make informed decisions about their personal information.[18]

We have also issued a call for cutting-edge research on a wide range of privacy and security issues to feature in our second PrivacyCon conference in January. Among other areas, we requested research on the use and effectiveness of opt-out mechanisms and other privacy controls, as well as on the development of tools to help businesses detect discrimination in algorithms.[19] The day after PrivacyCon, we will host a meeting of researchers and entities that fund research. Our aim is to highlight the need for privacy research and help researchers find the resources to explore new alternatives.

IV. Conclusion

To close, I want to emphasize once more that by focusing on the importance of consumer control, I am not suggesting that control alone is sufficient to address all of the privacy challenges we face today. Certainly, companies cannot put the onus on consumers to choose among basic privacy protections. Nor can they abdicate their responsibility to use reasonable measures to protect consumer data. Companies need to practice privacy and security-by-design, consider ethical issues in using big data, and refrain from collecting and storing consumer data that they do not need.

But I believe consumer control is a fundamental building block for privacy. Preferences among consumers may vary, and even a single consumer's preferences may vary, depending on context. The more sophisticated the tools consumers can have to express these preferences, the

[18] *See* Press Release, FED. TRADE COMM'N, FTC To Host September Workshop On Testing Effectiveness of Consumer Disclosures (May 24, 2016), https://www.ftc.gov/news-events/press-releases/2016/05/ftc-host-september-workshop-testing-effectiveness-consumer.
[19] *See* FED. TRADE COMM'N, PrivacyCon: Call for Presentations, https://www.ftc.gov/privacycon-call-for-presentations.

richer the interaction between consumers and businesses can be. I think this is a goal that is within our reach and urge companies to work toward it.

Thank you.