ConsumersUnion®
THE ADVOCACY DIVISION OF CONSUMER REPORTS

Statement of **Justin Brookman**
Director, Privacy and Technology Policy
Consumers Union

Before the House Subcommittee on Digital Commerce and Consumer Protection

Understanding the Digital Advertising Ecosystem

June 14, 2018

On behalf of Consumers Union, I want to thank you for the opportunity to testify today. We appreciate the leadership of Chairman Latta and Ranking Member Schakowsky in holding today's hearing to explore the digital advertising ecosystem and how digital advertisements affect Americans.

I appear here today on behalf of Consumers Union, the advocacy division of Consumer Reports, an independent, nonprofit, organization that works side by side with consumers to create a fairer, safer, and healthier world.[1]

[1] Consumer Reports is the world's largest independent product-testing organization. It conducts its advocacy work in the areas of privacy, telecommunications, financial services, food and product safety, health care, among other areas. Using its dozens of labs, auto test center, and survey research department, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 7 million members and publishes its magazine, website, and other publications.

Executive Summary

My testimony today is divided into three parts. First, I describe some of the many ways that the digital advertising ecosystem has gotten more complex in recent years, leaving consumers with little information or agency over how to safeguard their privacy. Consumers are no longer just tracked through cookies in a web browser: instead, companies are developing a range of novel techniques to monitor online behavior and to tie that to what consumers do on other devices and in the physical world. Next, I discuss industry adjustments in the face of rising consumer pressure, including Consumer Reports' own efforts to provide more accountability for and transparency of individual company practices. While some companies have reformed their offerings in response to consumer privacy concerns, ad tracking companies have by and large taken advantage of opacity and consumer confusion to evade scrutiny — and have backtracked from prior commitments to offer better protections. Finally, I conclude by recommending that this Committee consider practical legislative steps to give consumers better rights over their personal data and digital security. Consumers want more and better privacy protections, but do not have the practical ability to take action. Congress should explore various options to give individuals the protections they want and deserve.

I. Ad Tracking Has Become More and More Invasive

In recent years, ad tracking technologies have become incredibly sophisticated, with consumers monitored in a variety of ways they can neither detect nor control. Online tracking is no longer limited to "anonymous" cookies that monitor a web browser from site to site. Modern advertising companies track users by their real name, across multiple computers, and increasingly across other internet-connected devices and into the physical world.

In describing these evolving tracking practices, I do not mean to imply that they are universally bad methods, or that they should all be prohibited. But understanding the proliferation of tracking behaviors puts into context how increasingly difficult it is for individuals to exercise control over their personal information. Consumers are actively engaged online, spending around six hours per a day using digital media, mostly on mobile devices.[2] While some consumers may well appreciate receiving targeted offers, in study after study, the majority of people do not wish to be tracked in order to be served with more relevant advertising.[3] In a recent Pew Research study, 86% of users reported taking some action to mask their digital footprints, but most wish they had the ability to do more.[4] Older, less tech-savvy users especially feel powerless to take responsibility of protecting their privacy.[5] In the past, simply blocking cookies may have been sufficient to prevent the sort of online tracking that many consumers reject. Today, tracking takes many more

---

[2] Ginny Marvin, *Digital Advertising's Opportunities & Threats from Mary Meeker's Internet Trends Report*, MARKETING LAND (June 1, 2018), https://marketingland.com/digital-advertisings-opportunities-threats-from-mary-meekers-internet-trends-report-241264.

[3] Chris Jay Hoofnagle et al., *Privacy And Modern Advertising: Most US Internet Users Want 'Do Not Track' to Stop Collection Of Data About Their Online Activities*, AMSTERDAM PRIVACY CONFERENCE (Oct. 8, 2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2152135; Kristin Purcell et al., *Search Engine Use Over Time*, PEW RESEARCH CTR. (Mar. 9, 2012), http://www.pewinternet.org/2012/03/09/main-findings-11/; J. Turow et al., *Americans Reject Tailored Advertising And Three Activities That Enable It,* SSRN (2009), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[4] Lee Raine, *The State of Privacy In Post-Snowden America*, PEW RESEARCH CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

[5] Fatemeh Khatibloo, *Marketers, Here's How Your Customers Feel About Privacy*, FORBES (Dec. 16, 2016), https://www.forbes.com/sites/forrester/2016/12/16/marketers-heres-how-your-customers-feel-about-privacy/#52356c0f18e4.

forms, and is increasingly difficult to limit or control.

A. Real Name Tracking

Advertising companies previously defended online tracking because it was "anonymous" — digital companies didn't care *who* you were, they just wanted to market relevant products to unidentified users. In 2001, the Federal Trade Commission (FTC) closed an investigation into DoubleClick's merger with the data broker Abacus noting that: "DoubleClick did not combine PII [personally identifiable information] from Abacus Direct with clickstream collected on client Web sites."[6] Further, in 2008, in describing its "Commitment to Privacy in Online Advertising" to the U.S. Senate Commerce Committee, Microsoft explained that it relied on a de-identification process "to ensure that we use only data that does not personally identify individual consumers to serve ads online."[7]

Today, however, online tracking is no longer anonymous. In 2010, Facebook made available to publishers its now-ubiquitous "Like" buttons to embed into their web pages.[8] Because those buttons connect to Facebook directly even without any user interaction, Facebook is able to track registered users off of Facebook by their real names.[9] A recent study of leading websites determined that Facebook is embedded in approximately 69% of the those sites, giving Facebook broad insight into what people do off of their services.[10] Beginning in 2015, Facebook started to

---

[6] *Letter to DoubleClick*, FED. TRADE COMM'N (Jan. 22, 2001), https://www.ftc.gov/sites/default/files/documents/closing_letters/doubleclick-inc./doubleclick.pdf.
[7] *Statement of Michael D. Hintze, Before the U.S. Senate Comm. On Commerce, Sci. & Transp.*, MICROSOFT CORP., 15 (Jul. 9, 2008), available at https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00020/544506-00020.pdf.
[8] Tom Simonite, *Facebook's Like Buttons Will Soon Track Your Web Browsing to Target Ads*, MIT TECH REV. (Sept. 16, 2015), https://www.technologyreview.com/s/541351/facebooks-like-buttons-will-soon-track-your-web-browsing-to-target-ads/.
[9] Allen St. John, *How Facebook Tracks You, Even When You're Not on Facebook*, CONSUMER REPORTS (Apr. 11, 2018), https://www.consumerreports.org/privacy/how-facebook-tracks-you-even-when-youre-not-on-facebook/.
[10] Justin Brookman et al., *Cross-Device Tracking: Measurement and Disclosures*, PROCEEDINGS ON PRIVACY ENHANCING TECH. (2017), *available at* https://petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf.

use this data for ad targeting: thus, if Facebook tracked your shopping cart on a oline shoe seller site, it could later serve you an ad for shoes on Facebook (or possibly on a different site).[11] In 2016, Google followed suit and merged its logged-in user data with its third-party advertising data; for users who have signed into products such as Gmail or YouTube,

Google can now combine behavioral data collected off of Google through DoubleClick and other products with real name identity.[12] Google's penetration of the web is even greater than Facebook, appearing in over 87% of surveyed sites in one study.[13]

B. Cross-Device Tracking

Users typically log into Google and Facebook on different devices. As a result, those companies are able to monitor what you do around the web and in other apps on multiple devices — and to link all of that behavior together, tied to your identity.[14]

Other ad tracking companies may not have easy access to identifying information, but they increasingly use a variety of other tactics to try to correlate user behavior across different devices. Some many use *probabilistic* methods to identify devices that may share an owner based on shared attributes, such as internet protocol address. If two devices generally connect to the same local network, there is a decent chance they are used by the same individual. If they also exhibit similar browsing patterns (for example, the user on both devices tends to visit sites about the Washington

---

[11] *See Facebook's Like Buttons*, *supra* note 8.
[12] Julia Angwin, *Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking*, PROPUBLICA (Oct. 21, 2016), https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking.
[13] See *Cross-Device Tracking*, *supra* note 10. For a more extensive look at tracking on over one million of the top sites, *see* Steven Englehardt & Arvind Narayanan, *Online Tracking: A 1-Million-Site Measurement and Analysis*, PRINCETON WEB CENSUS (2016), http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf; Russell Brandom, *Google And Facebook Still Dominate Tracking on The Web*, THE VERGE (May 18, 2016), https://www.theverge.com/2016/5/18/11692228/google-facebook-web-tracking-survey-advertising.
[14] *See Cross-Device Tracking: An FTC Report*, FED. TRADE COMM'N, 2-3 (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.

Capitals and technology law), they are even more likely to share an owner.[15]

Some companies receive identifying information from publishers that collect login information. If you provide your email address or username to a website to log into a service, that service may share that identifying information with various ad tracking companies. If a tracking company receives the same identifiers across multiple devices, it is able to generate a *deterministic* cross-device profile of the user.[16]

Furthermore, some companies have experimented with other technologies such as ultrasonic audio beacons to track users across devices. Audio beacons are inaudible signals that are played through a speaker on a connected device like a computer, tablet, or TV. If an ultrasonic code is played in the vicinity of a device that has software in an app or other platform that can listen for the inaudible code, the listening device will then identify that the same individual has used both devices and thereby enable an advertiser to more accurately track a user across devices.[17] Advertisers have also embedded software in apps that would enable companies to know what a user is watching on their TV by listening through the device's microphone. This information can then be added to a profile about a user and used to create targeted advertisements for the individual. In early 2016, the FTC issued warning letters to developers who installed audio beacon software in apps in order to listen for inaudible signals to log what users watched on TV.[18] Despite this warning, other developers like Alphonso have continued to make use of similar technologies in order to track users across different devices and served targeted ads.[19]

---

[15] *Id*. at 3.
[16] For a more detailed discussion of these methods, *see, generally, Cross-Device Tracking, supra* note 8.
[17] *Comments for November 2015 Workshop on Cross-Device Tracking*, CTR. FOR DEMOCRACY & TECH. (Oct. 16, 2015), https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf.
[18] *FTC Issues Warning Letters to App Developers Using 'Silverpush' Code*, FED. TRADE COMM'N (Mar. 17, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code.
[19] Sapna Maheshwari, *That Game on Your Phone May Be Tracking What You're Watching On TV*, N.Y. TIMES (Dec. 28, 2017), https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html. According to

C. *Internet of Things*

More and more of the objects we use and purchase are technology- and internet-enabled. Cars, televisions, home assistants, and even kitchen appliances have the ability to go online to expand the functionality of those products. At the same time, ad tracking companies can leverage the information generated by these devices to expand a marketing profile about a user — often without a great deal of transparency.

Smart televisions are a good example. Many smart TVs use a technology called "automated content recognition" (ACR) to collect and transmit screenshots from the TV in order to determine what types of content the household is watching. In 2015, the FTC reached a settlement with the manufacturer Vizio over its use of ACR to track the television viewing habits of consumers without clear permission.[20] Consumer Reports published the results of its own investigation of smart TV behavior earlier this year, finding that all the major TV manufacturers examined used ACR to monitor owners' use of their products (with varying degrees of transparency and control).[21]

Voice assistants in the home like Amazon's Echo, Sonos's One, and Google's Home present further possibilities for tracking, though advertisers have not fully realized the opportunity to reach consumers via these new sources yet.[22] Adoption of these devices is expected to reach the

---

the *New York Times* report, Alphonso used a different type of technology in order to determine what shows users were listening, similar to the automated content recognition described in the following section used by smart televisions.

[20] *Vizio to Pay $2.2 Million to FTC, State of New Jersey To Settle Charges It Collected Viewing Histories On 11 Million Smart Televisions Without Users' Consent*, FED. TRADE COMM'N (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

[21] *Samsung And Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds*, CONSUMER REPORTS (Feb. 7, 2018), https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/. The *Consumer Reports* study also found security vulnerabilities in two of the televisions that would allow hackers to manipulate the television remotely to, for example, set the volume to maximum, or display offensive content.

[22] *See Digital Advertising's Opportunities*, *supra* note 2.

majority (55%) of all U.S. households by 2022.[23] These devices may well expand data collection capacity and facilitate the delivery of targeted advertisements. Advertising through voice assistants would also present additional challenges to transparency, as consumers will not have visual indicators that particular recommendations are paid advertisements and may have less opportunity to learn about and control the way their data is collected and used.

D. The Constant Proliferation of Tracking Technologies

The methods described above are just a subset of some of the new tactics that companies use to track and target consumers. But the list is far from exhaustive. Other examples include: tailoring of online ads based on in-store purchases,[24] the collection of cell phone signals to generate in-store retail analytics,[25] internet service provider monitoring of user behavior for ad targeting,[26] and email targeting based simply on visiting a website[27] or making a purchase at a retail location.[28] Academic researchers at institutions such as Princeton, Northeastern, and the University of California have researched and cataloged many of these behaviors,[29] but it is next to impossible

---

[23] Sarah Perez, *Voice-Enabled Smart Speakers to Reach 55% Of U.S. Households By 2022, Says Report*, TECHCRUNCH (Nov. 8, 2017), https://techcrunch.com/2017/11/08/voice-enabled-smart-speakers-to-reach-55-of-u-s-households-by-2022-says-report/.

[24] Tim Peterson, *Facebook Will Target Ads to People Based on Store Visits, Offline Purchases, Calls to Businesses*, MARKETING LAND (Sept. 21, 2017), https://marketingland.com/facebook-will-target-ads-people-based-store-visits-offline-purchases-calls-businesses-224668.

[25] Siraj Datoo, *How Tracking Customers In-Store Will Soon Be the Norm*, THE GUARDIAN (Jan. 10, 2014) https://www.theguardian.com/technology/datablog/2014/jan/10/how-tracking-customers-in-store-will-soon-be-the-norm.

[26] Jon Brodkin, *How ISPs Can Sell Your Web History—And How to Stop Them*, ARS TECHNICA (Mar. 24, 2017), https://arstechnica.com/information-technology/2017/03/how-isps-can-sell-your-web-history-and-how-to-stop-them/

[27] Jess Nelson, *Criteo Launches Dynamic Email Retargeting Solution*, MEDIAPOST (May 20, 2016) https://www.mediapost.com/publications/article/276266/criteo-launches-dynamic-email-retargeting-solution.html.

[28] Ben Popper, *Square Adds Marketing Tools So Merchants Can Email Their Customers*, THE VERGE (Apr. 7, 2015), https://www.theverge.com/2015/4/7/8359483/square-marketing-email-promotions.

[29] *See*, *e.g.*, PRINCETON WEB TRANSPARENCY AND ACCOUNTABILITY PROJECT, https://webtap.princeton.edu/ (last visited June 12, 2018). For the past three years, the Federal Trade Commission has held *PrivacyCon* to hear from cutting edge privacy researchers in order to educate itself and the policy community about some of these latest tracking techniques. *See* FED. TRADE COMM'N'S PRIVACYCON 2018 (last visited June 12, 2018), https://www.ftc.gov/news-events/events-calendar/2018/02/privacycon-2018.

for ordinary consumers to learn about how they are being monitored, or take control of their personal information. Indeed, many privacy violations are completely unobservable by consumers. For instance, if personal data stored with a cloud provider is transmitted to someone else, consumers have no visibility into that transmission. If the data is accessed inadvertently or maliciously, the provider may have obligations to disclose to consumers under breach notification laws. However, if the transmission is intentional — that is, if the provider deliberately provides data to a third-party — a consumer would have no way to detect that disclosure of their information.

Persistent confusion — even among experts — about whether and how connected products and services can listen to personal conversations illustrates the challenges for consumers.[30] Just last week, Vice published a story purporting to prove that Facebook listens to ambient conversations for ad targeting purposes.[31] Privacy researchers cast doubt on the story, but the fact that leading authorities cannot even agree on whether Facebook is mining personal audio conversations is emblematic of the generalized confusion about privacy in a world of connected sensors. When sophisticated technology reporters cannot figure out how their personal information is collected and used,[32] the challenge for average consumers — worried about privacy but without the time or training to protect themselves — becomes clear. And the public is left feeling frustrated and helpless.

---

[30] David Goldman, *Your Samsung TV Is Eavesdropping on Your Private Conversations*, CNN (Feb. 10, 2015), http://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/index.html.
[31] Sam Nichols, *Your Phone Is Listening and It's Not Paranoia*, VICE (June 4, 2018), https://www.vice.com/en_uk/article/wjbzzy/your-phone-is-listening-and-its-not-paranoia.
[32] *See*, *e.g.,* Kashmir Hill, *Facebook Figured Out My Family Secrets and It Won't Tell Me How*, GIZMODO (Aug. 25, 2017), https://gizmodo.com/facebook-figured-out-my-family-secrets-and-it-wont-tel-1797696163; JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE (2014).

II. Some Companies are Responding to Market Pressure, but Industry Self-Regulation Has Failed to Date

Unfortunately, digital advertising is still largely opaque to the consumer who is tracked both on- and off-line. Consumers feel like they lack control over how often their personal information is shared and how much digital advertisers know about them.

In response to these concerns, some market actors have made significant changes to limit data collection on their platforms. For example, Apple, in 2013 introduced a mandatory "Limit Ad Tracking" setting for iPhone applications, and recently improved that tool to further limit the information advertisers can receive when the setting is activated.[33] Mozilla too has taken efforts to differentiate its Firefox web browser by adopting policies to limit cross-site data collection.[34] Services like DuckDuckGo have found some success in marketing themselves as the tracking-free alternative to larger search engine companies that rely on data for advertising.[35] And a number of private entities have developed ad blockers that stop many online tracking techniques, such as Disconnect.me, the Electronic Future Foundation's Privacy Badger, and uBlock. Industry analysts expect ad blocker adoption to reach 30% this year, led primarily by the youngest internet users.[36] The start-up Brave has also developed browsers that block ads by default, and is exploring alternative web funding models based on privacy-friendly ads and micropayments of cryptocurrency.[37]

---

[33] Lara O'Reilly, *Apple's Latest iPhone Software Update Will Make It A Lot Harder for Advertisers to Track You,* BUS. INSIDER (Sept. 10, 2016), http://www.businessinsider.com/apple-ios10-limit-ad-tracking-setting-2016-9.
[34] Monica Chin, *Firefox's Quantum update will block websites from tracking you 24/7*, MASHABLE (Jan. 23, 2018), https://mashable.com/2018/01/23/firefox-quantum-releases-update/#yPrZ0O74MqqQ.
[35] Apekshita Varshney, *Hey Google, DuckDuckGo Reached 25 Million Daily Searches*, TECHWEEK (June 4, 2018), https://techweek.com/search-startup-duckduckgo-philadelphia/.
[36] *30% of All Internet Users Will Ad Block By 2018*, BUS. INSIDER (Mar. 21, 2017), http://www.businessinsider.com/30-of-all-internet-users-will-ad-block-by-2018-2017-3.
[37] Stephen Shankland, *Ad-Blocking Brave Browser to Give Crypto-Payment Tokens to Everyone*, CNET (Apr. 19, 2018), https://www.cnet.com/news/ad-blocking-brave-browser-to-give-crypto-payment-tokens-to-everyone/.

For its part, Consumer Reports is taking steps to provide more accountability for the market and to give consumers actionable information about which companies do a better job of protecting user privacy. To help consumers make decisions in the marketplace, Consumer Reports has developed, and is actively testing products under, the Digital Standard. The Digital Standard[38] is an open standard for testing products and services for privacy and security. Our testing under the Standard includes assessments of a company's stated privacy practices in both the user interfaces and in their privacy policies, as well as analysis of traffic flows. And it examines such questions as: Does the company tell the consumer what information it collects? Does it only collect information needed to make the product or service work correctly? And does the company explicitly disclose every way it uses the individual's data?[39] While we are currently conducting case studies under the Standard to ensure that the process is scientific and repeatable, we plan to eventually include privacy and digital security in our comparative testing of products where there is potential market differentiation. Our ultimate goal is to enable consumers to make better, more informed privacy choices, and to spur improvements and greater competition among companies on privacy.

Despite some market improvements, as discussed above, tracking technology has gotten more invasive in recent years. Moreover, industry efforts to self-regulate have largely failed. Five years ago, I testified about the various weaknesses in ad tracking self-regulatory programs: the rules only apply to coalition members; industry opt-outs are fragile and easily overridden; industry opt-outs only address usage and do not impose meaningful collection or retention limitations; and

[38] The Digital Standard (theDigitalStandard.org) was launched on March 6, 2017 and is the result of a collaboration with our cybersecurity partners, Disconnect, Ranking Digital Rights, and the Cyber Independent Testing Lab. The Standard is designed to hold companies accountable and equip Consumer Reports and other organizations to test and rate products for how responsibly they handle our private data. This is a collaborative and open source effort. The Standard is designed to empower consumers to make informed choices about the connected products, apps, and services consumers use everyday.
[39] *Id*.

notice and privacy interfaces were seriously flawed.[40] These criticisms largely remain intact today, before even considering the dramatic expansion of tracking technologies in recent years.

Industry had originally committed to addressing these flaws by adopting the Do Not Track web standard to give consumers a more robust opt-out tool. In 2012, industry representatives committed to honoring Do Not Track instructions at a White House privacy event.[41] Over the next few years, however, as regulatory pressure and the prospect of new legislation faded, industry backed away from its commitment, with trade groups publicly announcing withdrawal from the industry standard process at the World Wide Web Consortium.[42] Today, seven years after Do Not Track settings were introduced into all the major browser vendors, few ad tracking companies meaningfully limit their collection, use, or retention of consumer data in response to consumers' Do Not Track instructions.

III. American Consumers Deserve Stronger Privacy Rights Under the Law

Consumers Union and Consumer Reports are committed to improving transparency and incentivizing the market to sufficiently protect personal information through product testing under the Digital Standard. However, ultimately, U.S. consumers need stronger privacy laws to give users greater rights and protections in a world of universal surveillance and connectivity.[43] Such a law should require:

---

[40] *Statement of Justin Brookman Before the U.S. Senate Comm. On Commerce, Sci., and Transp.*, CTR. FOR DEMOCRACY & TECH. (Apr. 24, 2013), https://cdt.org/files/pdfs/Brookman-DNT-Testimony.pdf.
[41] Dawn Chmieleski, *How 'Do Not Track' Ended Up Going Nowhere,* RECODE (Jan. 4, 2016), https://arstechnica.com/information-technology/2017/03/how-isps-can-sell-your-web-history-and-how-to-stop-them/; *see* Julia Angwin, *Web Firms to Adopt 'No Track' Button*, WALL ST. J. (Feb. 23, 2012), https://www.wsj.com/articles/SB10001424052970203960804577239774264364692.
[42] Kate Kaye, *Do-Not-Track on The Ropes as Ad Industry Ditches W3C*, ADAGE (Sept. 17, 2013), http://adage.com/article/privacy-and-regulation/ad-industry-ditches-track-group/244200/.
[43] Jessica Rich, *Beyond Facebook, It's High Time for Stronger Privacy Laws*, WIRED (Apr. 8, 2018), https://www.wired.com/story/beyond-facebook-its-high-time-for-stronger-privacy-laws/.

- Clear, easy-to-understand and compare information about data practices;
- Simple and easy-to-use consumers choices;
- The collection and retention of only the data necessary — and the disposal of old data;
- Strong data security practices;
- Ways for consumers to get easy access to their information; and
- A strong enforcement cop to ensure accountability.[44]

Unfortunately, legal protections at the federal level are — if anything — getting weaker.[45] Just last week, an appeals court further constrained the FTC's already limited authority to order companies to cease bad data security practices.[46] Currently, it is the states that are advancing legislation to safeguard consumer privacy and security. For example, a ballot initiative in California this November may establish mandatory transparency and opt-out requirements around the sale of personal information to third-party data brokers.[47] Just as states have determined the legal landscape for data breach notification,[48] states seem poised to set more comprehensive standards for security and data privacy. While Consumers Union supports many of these state legislative initiatives, a strong, consistent federal law ensuring privacy and security protections for all personal data is still needed. We urge this Committee to hold further hearings on this issue, with a focus on how legislation can balance individual liberty and agency with the need to account for future technologies and innovation.

---

[44] *Where We Stand: Congress Should Pass A Strong Privacy Law, Now*, CONSUMER REPORTS (Apr. 9, 2018), https://www.consumerreports.org/privacy/its-time-for-congress-to-pass-a-strong-privacy-law/.
[45] Justin Brookman, *Protecting Privacy in An Era of Weakening Regulation*, HARV. L. & POL'Y REV., Vol. 9 (2015), *available at* http://harvardlpr.com/wp-content/uploads/2015/07/9.2_3_Brookman.pdf.
[46] Alison Frankel, *There's A Big Problem for The FTC Lurking in the 11th Circuit's LabMD Data-Security Ruling*, REUTERS (June 7, 2018), https://www.reuters.com/article/us-otc-labmd/theres-a-big-problem-for-the-ftc-lurking-in-11th-circuits-labmd-data-security-ruling-idUSKCN1J32S2.
[47] Daisuke Wakabayaski, *Silicon Valley Faces Regulatory Fight on Its Home Turf*, N.Y. TIMES (May 13, 2018), https://www.nytimes.com/2018/05/13/business/california-data-privacy-ballot-measure.html.
[48] *Data Breach Notification Laws: Now in All 50 States*, PRIVACY RIGHTS CLEARINGHOUSE (May 9, 2018), https://www.privacyrights.org/blog/data-breach-notification-laws-now-all-50-states.

Conclusion

Thank you again for the opportunity to testify here today about the state of the digital advertising marketplace and the need for strong consumer controls over how their data is collected and used. I look forward to answering the Committee's questions.