Statement of Laura Moy
Associate Professor of Law, Georgetown University Law Center
Director, Communications & Technology Law Clinic
Associate Director, Center on Privacy & Technology

Before the

United States Senate
Committee on Commerce, Science, and Transportation

Hearing on

Examining Legislative Proposals to Protect Consumer Data Privacy

Wednesday, December 4, 2019

Please contact Laura Moy at laura.moy@georgetown.edu with questions.

Introduction and Summary

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, thank you for inviting me here today. I am Laura Moy, an associate professor at Georgetown Law and director of the law school's Communications & Technology Law Clinic. I appreciate the opportunity to testify today on consumer privacy. I make six points:

1. **Congress must accept that a strong consumer privacy law will force business practices to change.** That change will be costly for companies. Companies may protest a strong privacy law, but Congress should take its lead from people, not companies. Congress should accept that meaningful regulation requires an adjustment period.

2. **Privacy legislation must contain use restrictions.** It is not enough to require companies merely to disclose what they plan to do with consumer data; rather, they should be restricted to uses that are reasonable. And some applications of consumer data should simply be off-limits.

3. **Congress must not accept legislation without civil rights protections.** The most troubling use of data is to facilitate discrimination. Congress should prohibit uses of data that selectively deny access to—or awareness of—opportunities in housing, education, finance, employment, and healthcare.

4. **Congress should not step on states' toes.** As Congress considers establishing new privacy and data security protections for Americans' private information, it should *not* eliminate existing protections that already benefit Americans at the state level. Nor should it preempt the states' right to develop new ways to protect their citizens. States are innovating in this space right now and making valuable contributions.

5. **There are valuable provisions in multiple bills before this committee.** The Committee should be commended for working diligently and creatively to develop legislation that meets growing demands for privacy protection.

6. **If Congress cannot agree on legislation that embodies the Public Interest Privacy Legislation Principles, it should not act.** One option before Congress is to hold its pen. If Congress cannot produce a bipartisan bill that synthesizes the valuable provisions across bills to embody the principles advanced by public interest organizations over a year ago, perhaps it should wait—and allow states to continue to fill the gap.

1. We need regulation that changes the industry

As Congress considers how best to address calls for consumer privacy protections, it should not shy away from major reforms. Congress must accept that a strong consumer privacy law will force business practices to change, and that will be costly for companies. But major change is necessary, both to address consumers' longstanding unanswered privacy concerns and to rein in harmful misuses of consumer data that should never have been allowed to become entrenched.

According to a recent poll, a majority of Americans now feel that "the threat to personal privacy online is a crisis, and we need forced changes to the way companies operate."[1] Americans overwhelmingly feel they have no control and little understanding about how their information is used. Following a large survey of thousands of U.S. adults, Pew Research Center reported in November that 81% say they have very little or no control over the data companies collect and 59% have very little or no understanding about what companies do with the data collected.[2] At the same time, Americans plainly have deep privacy concerns, with the survey revealing that:

- 81% feel the potential risks of companies collecting data about them outweigh the benefits;
- 72% say they personally benefit very little or none from companies collecting data about them; and
- 79% are very or somewhat concerned about how companies use the data collected.[3]

---

[1] Laura Wronski, *Axios/SurveyMonkey Poll: Privacy Deep Dive*, Mar. 9, 2019, https://www.surveymonkey.com/curiosity/surveymonkey-axios-poll-privacy-deep-dive/.

[2] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, & Erica Turner, Pew Research Center, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, Nov. 15, 2019, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[3] *Id.*

These privacy concerns are distributed across industries. A whopping 85% of Americans are concerned a lot or a little about how much personal information social media sites know about them, 84% about advertisers, and 80% about companies they buy things from.[4]

Americans also have a striking lack of trust in companies' ability and incentives to address this problem:

- 69% are not too confident or not at all confident that firms will use their personal information in ways they will be comfortable with;
- 79% are not too confident or not at all confident that companies will admit mistakes and take responsibility if they misuse or compromise personal information; and
- 57% are not too confident or not at all confident that companies follow what their privacy policies say they do with users' personal data.[5]

And Americans agree that government needs to do more to address this problem. According to the same Pew survey, 75% of U.S. adults say there should be more regulation than there is now. That includes both Republicans (70%) and Democrats (81%).[6]

In the absence of robust regulation, although providers of online sites and services often engage in ongoing conversations with civil rights, civil liberties, and public interest groups, they nevertheless have repeatedly failed to respect and protect data relating to millions—and at times billions—of users. In recent years the lack of strong privacy protections has led to countless highly publicized failures such as when Cambridge Analytica successfully used Facebook's platform to learn private information about many more than 87 million users, and when Google revealed that it was still tracking users' location through use of its services even after users had disabled the "Location History" feature.[7]

---

[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] Chaim Gartenberg, *Google Updated its Site to Admit It Still Tracks You Even if You Turn Off Location History*, The Verge, Aug. 17, 2018, https://www.theverge.com/2018/8/17/17715166/google-location-tracking-history-weather-maps.

2. Privacy legislation must contain use restrictions

Many of our privacy laws in past years have been based on a notice and consent (or "transparency and control") framework—the idea that companies should be able to do what they please with consumer data so long as they are open about it and get permission. But it is time to recognize we need more, and to adopt meaningful use restrictions. Some uses of data are clearly harmful. In addition, consumers can no longer easily understand what they are disclosing when they share information online. The consent model also has reached the limits of scalability and is no longer feasible as a practical matter.

Consumers and policymakers alike now recognize a wide range of harms from certain data-driven content distribution models. On many platforms and services, consumer data is used to predict what advertisements, products, or other content a consumer will like or otherwise engage with so that they can be shown that information, for the purpose of maintaining their interest and generally holding them on the service for as long as possible. There are obvious incentives for companies to employ this model, under theories that 1) it is more efficient to show a consumer something she is interested in rather than waste computing power showing her something irrelevant to her, and 2) it is beneficial to keep a consumer's interest for as long as possible for the purpose of displaying more ads, products, or other content to her. But many consumers object to data-driven personalization. According to a 2019 privacy and security survey conducted by security company RSA:

- Only 31% of U.S. respondents believe that tailored newsfeeds are ethical;
- Only 37% believe that it's ethical to make recommendations to a user based on purchase/browsing history; and
- Only 38% believe that using a "like" history to recommend content is ethical.[8]

Consumers are concerned about data-driven distribution models with good reason. There is growing information that these models can lead to a

[8] RSA, *RSA Data Privacy & Security Survey 2019: The Growing Data Disconnect Between Consumers and Businesses* (2019), https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf.

number of harms not only to individual consumers, but to society more broadly. For example, these models can lead to:

- Widening political polarization. Data-driven models may be more likely to promote hyper-partisan content, which in turn may exacerbate political polarization. As one prominent legal scholar has written, "Self-insulation and personalization are solutions to some genuine problems, but they also spread falsehoods, and promote polarization and fragmentation."[9]
- Dissemination of propaganda, misinformation, and disinformation. Consumer data may be used to generate and target false information, including state-sponsored propaganda, careless or low-quality reporting, and false information designed to undermine democracy.[10]
- Amplification of hate speech. Consumer data may also be used to make the distribution of hateful and racist rhetoric and calls to violence more efficient.[11]
- Public health threats. Data-driven models that equate user "engagement" with success may be designed to be addictive and inescapable.[12] Addiction to social media and other services can lead to

---

[9] Cass R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media* at 5 (2017).

[10] David McCabe, *Facebook Finds New Coordinated Political Disinformation Campaign*, Axios, July 31, 2018, https://www.axios.com/facebook-finds-misinformation-campaign-4c5910b3-021a-45b7-b75c-b1ac80cbce49.html; Dipayan Ghosh & Ben Scott, *Disinformation Is Becoming Unstoppable*, Time, Jan. 24, 2018; April Glaser & Will Oremus, *The Shape of Mis- and Disinformation*, Slate, July 26, 2018, https://slate.com/technology/2018/07/claire-wardle-speaks-to-if-then-about-how-disinformation-spreads-on-social-media.html; Alice Marwick & Rebecca Lewis, *Media Manipulation and Disinformation Online* (2017), https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf.

[11] *See* Ariana Tobin, Madeleine Varner, & Julia Angwin, *Facebook's Uneven Enforcement of Hate Speech Rules Allows Vile Posts to Stay Up*, ProPublica, Dec. 28, 2017, https://www.propublica.org/article/facebook-enforcement-hate-speech-rules-mistakes; Swathi Shanmugasundaram, Southern Poverty Law Center, *The Persistence of Anti-Muslim Hate on Facebook* (May 5, 2018), https://www.splcenter.org/hatewatch/2018/05/05/persistence-anti-muslim-hate-facebook.

[12] Center for Humane Technology, *The Problem*, http://humanetech.com/problem/ (last visited Oct. 7, 2018) (explaining that operators of online

a cascade of other problems, including heightened rates of depression, suicide, and sleep deprivation among young people.[13]

- Distribution of discriminatory advertisements. Data-driven ad distribution can result in information about critical opportunities being systematically withheld from entire classes of people.[14]

Use restrictions may not be able to prevent all of these harms entirely, but should prohibit at least the most egregious misuses of data, as well as create obligations for companies that employ data-driven distribution models to detect problems such as those described here and take steps to address them.

Use restrictions are also needed because meaningful consent is no longer feasible in all circumstances as a practical matter.[15] There are too

---

services competing for users' attention are constantly learning how better to "hook" their users, and designing products intentionally to addict users).

[13] Recent studies have linked the use of platforms like Facebook, Snapchat, and Instagram to depressive symptoms in young adults caused by negatively comparing oneself to others on social media platforms. Brian A. Feinstein, et al., *Negative Social Comparison on Facebook and Depressive Symptoms: Rumination as a Mechanism*, 2 Psych. Pop. Media Culture 161 (2013). http://psycnet.apa.org/record/2013-25137-002. Experts have also found that teens who spend three hours a day or more on electronic devices are 35 percent more likely to have a risk factor for suicide and 28 percent more likely to get less than seven hours of sleep. Jean M. Twenge, *Have Smartphones Destroyed a Generation?*, The Atlantic, Sept. 2017, https://www.theatlantic.com/magazine/archive/2017/09/has-the-smartphone-destroyed-a-generation/534198/. Data-driven content distribution has also led to the proliferation of dangerous health-related misinformation. *See, e.g.*, Christine Hauser, *Drinking Bleach Won't Cure Autism or Cancer, F.D.A. Says*, N.Y. Times, Aug. 13, 2019, https://www.nytimes.com/2019/08/13/health/drinking-bleach-autism-cancer.html (the FDA was forced to counter medical misinformation telling consumers to drink bleach solutions as cures for autism, cancer, H.I.V./AIDS, and other conditions).

[14] *See generally* Muhammad Ali, Piotr Sapiezynski, Miranda Bogen, Aleksandra Korolova, Alan Mislove, & Aaron Rieke, *Discrimination Through Optimization: How Facebook's Ad Delivery Can Lead to Skewed Outcomes*, Proceedings of the ACM on Human-Computer Interaction (2019), https://arxiv.org/abs/1904.02095 [hereinafter *Discrimination Through Optimization*].

[15] There is a lengthy discussion of this problem in the testimony of Professor Woodrow Hartzog before this Committee earlier this year. *See* Prepared Testimony and Statement for the Record of Woodrow Hartzog before the Senate Committee on Commerce, Science, and Transportation regarding

many data exchanges every single day for consumers realistically to understand all of them and read every privacy policy.[16] And as we become surrounded by always-on connected devices, it is increasingly difficult for companies to solicit and receive consent. It remains important for companies to be transparent about their practices and to be required to observe user rights attaching to consumer data, but use restrictions would provide a much-needed backstop to protect against inappropriate uses of data.

In addition, use restrictions are needed because it has become exceptionally difficult for consumers to understand what they are disclosing when they share information online. Today, very sensitive information about a consumer can be inferred from data that seems less sensitive. For example:

- Cell phone sensors might be used to infer whether or not someone has Parkinson's;[17]
- Data about brushing habits collected by a person's toothbrush app might be used to infer health status, travel patterns, and relationship status;[18] and

---

"Policy Principles for a Federal Data Privacy Framework in the United States (Feb. 27, 2019), *available at* https://www.commerce.senate.gov/services/files/8B9ADFCC-89E6-4DF3-9471-5FD287051B53.

[16] *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S:J. L. & Pol'y for Info. Soc'y 1, 9 (2008), http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf (estimating the national opportunity cost for the time it would take Americans to read every privacy policy they come across at $781 billion);Joel R. Reidenberg, N. Cameron Russell, Alexander J. Callen, Sophia Qasir, & Thomas B. Norton, *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S: A Journal of Law and Policy 485, 492 (2014) ("To start, there are simply too many privacy policies to keep track of, given the potentially hundreds of websites a user might visit on any given day. To read all of these privacy policies would be extremely time consuming and extremely costly.").

[17] Ana de Barros, *Parkinson's DREAM Challenge Uses Mobile Sensor Data to Monitor Health Based on Movement*, Parkinson's News Today, July 20, 2017, https://parkinsonsnewstoday.com/2017/07/20/parkinsons-digital-dream-challenge-uses-smartphones-remote-sensing-data-monitor-health/.

[18] *See* Justin Peters, *Should This Thing Be Smart? Toothbrush Edition.*, Slate, Mar. 12, 2018, https://slate.com/technology/2018/03/should-this-thing-be-smart-colgate-connect-e1-smart-toothbrush-edition.html.

- Location data might be used to infer where a person works, lives, and worships, where their kids go to school, and the facility where they seek medical treatment.[19]

This Committee should seek to further develop use restrictions in privacy legislation. Two bills before the Committee contain provisions that serve as good starting points. The Consumer Online Privacy Rights Act (COPRA) introduced just last week by Ranking Member Cantwell and Senators Schatz, Klobuchar, and Markey, as well as the Privacy Bill of Rights Act introduced by Senator Markey, prohibit discriminatory uses of data as described above, as well as certain uses of biometric information.[20]

Notice and consent has clear limits. For privacy legislation to protect consumers, it must contain meaningful use limitations as well.

3. Congress must not accept legislation that does not contain civil rights protections

Congress should reject out of hand any consumer privacy proposal that does not contain civil rights protections. If Congress is going to legislate, it should legislate for all consumers. One important way to do this is to ensure that consumer data cannot be used to facilitate discrimination or otherwise to selectively deny access to—or awareness of—critical opportunities in housing, education, finance, employment, and healthcare.

Indeed, the public interest community has been consistent in its insistence that antidiscrimination must be a part of any consumer privacy law. The Public Interest Privacy Legislation Principles signed by 34 organizations in November 2018 state, "Automated decision-making, including in areas such as housing, employment, health, education, and lending, must be judged by its possible and actual impact on real people, must operate fairly for all communities, and must protect the interests of the

---

[19] *See* Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times, Dec. 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[20] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019) (as introduced by S. Cantwell to the S. Comm. on Commerce, Sci., and Transp.); Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019) (as introduced by S. Markey).

disadvantaged and classes protected under anti-discrimination laws."[21] In February, 47 organizations sent a letter to this Committee that stated in part,

> Civil rights protections have existed in brick-and-mortar commerce for decades. It is time to ensure they apply to the internet economy as well. Online services should not be permitted to use consumer data to discriminate against protected classes or deny them opportunities in commerce, housing, employment, or full participation in our democracy. Congress should require companies to be transparent about their collection and use of personal information in automated decision-making. Companies must also anticipate and protect against discriminatory uses and disparate impacts of data.[22]

In April, many of those organizations sent this Committee a follow-up letter reiterating the importance of centering civil rights concerns and urging Congress to:

1) Prohibit the use of personal data to discriminate in employment, housing, credit, education, or insurance—either directly or by disparate impact.
2) Prohibit the use of personal data to discriminate in public accommodations and extend such protections to businesses that offer goods or services online.
3) Prohibit the use of personal data to engage in deceptive voter suppression.
4) Require companies to audit their data processing practices for bias and privacy risks.
5) Require robust transparency at two tiers: easy-to-understand privacy notices for consumers, and comprehensive annual privacy reports for

---

[21] *Public Interest Privacy Legislation Principles*, Nov. 2018, https://newamericadotorg.s3.amazonaws.com/documents/Public_Interest_Privacy_Principles.pdf.

[22] The Leadership Conference on Civil & Human Rights, *Over 40 Civil Rights, Civil Liberties, and Consumer Groups Call on Congress to Address Data-Driven Discrimination*, Feb. 13, 2019, https://civilrights.org/2019/02/13/over-40-civil-rights-civil-liberties-and-consumer-groups-call-on-congress-to-address-data-driven-discrimination/.

researchers and regulators. Companies must completely disclose how they collect and use personal data, including their algorithmic processing practices.

6) Enable researchers to independently test and audit platforms for discrimination.
7) Empower a federal agency with rulemaking authority, enforcement powers, and enough resources to address current and future discriminatory practices.
8) Provide individual rights to access, correct, and delete one's personal data and inferences made using that data.
9) Provide a private right of action. Marginalized communities historically have not been able to rely upon the government to protect their interests, so individuals need to be able to vindicate their own rights.
10) Establish baseline nationwide protections and allow states to enact stricter laws. Under no circumstances should Congress enact any legislation that could preempt state civil rights laws, many of which are stronger than federal law. For example, many states extend greater antidiscrimination protections to the LGBTQ+ community than federal law.[23]

Congress must honor these requests from the public interest community because at present, these impermissible uses of information are widespread. For example, Facebook made assurances in 2017 to tackle discriminatory advertising on its platform after facing public outrage and pressure from advocates regarding its "ethnic affinity" advertising clusters, but the Washington State Attorney General later found that it was still possible to exclude people from seeing advertisements based on protected class membership.[24] Earlier this year civil rights organizations settled lawsuits with Facebook over charges that the platform enabled landlords and

---

[23] Letter from 26 civil society organizations to House and Senate Commerce Committees calling for prioritization of civil rights considerations in privacy legislation, Apr. 19, 2019, https://newamericadotorg.s3.amazonaws.com/documents/Letter_to_Congress_on_Civil_Rights_and_Privacy_4-19-19.pdf.
[24] Sam Machkovech, *Facebook Bows to WA State to Remove "Discriminatory" Ad Filters*, Ars Technica, July 25, 2018, https://arstechnica.com/information-technology/2018/07/facebook-bows-to-wa-state-pressure-to-remove-discriminatory-ad-filters/.

real estate brokers to exclude families with children, women, and other protected classes of people from receiving housing ads, and also facilitated gender discrimination in job ads.[25]

The systematic targeting and exclusion of communities can be a byproduct of algorithmic content and ad distribution that optimizes for cost-effectiveness and user "engagement," which can lead to distribution that is discriminatory in impact, if not intent.[26] For example, this year a team of researchers found that when sponsored employment ads were posted on Facebook for a wide range of positions, including janitors, nurses, lawyers, the platform's algorithms delivered ads in a way that demonstrated clear race and gender bias.[27] More specifically, the platform displayed ads for jobs in the lumber industry to an audience that was 72% white and 90% men, for supermarket cashier positions to 85% women, and for jobs with taxi companies to 75% black users. This type of discriminatory outcome occurred even though the advertisers never specified a demographic audience for the ads.

To prevent these types of unacceptable outcomes, any new privacy legislation should outright prohibit the use of consumer data to facilitate discrimination, and also should force companies to conduct their own forecasting and testing to determine whether discrimination is occurring on their platform or is likely to occur.

Multiple bills attempt to deliver in this area. COPRA is the only bill before this committee that would both prohibit discriminatory uses of data

---

[25] Communications Workers of America, *Facebook Agrees to Sweeping Reforms to Curb Discriminatory Ad Targeting Practices* (Mar. 19, 2019), https://cwa-union.org/news/releases/facebook-agrees-sweeping-reforms-curb-discriminatory-ad-targeting-practices.

[26] *See* Anja Lambrecht & Catherine E. Tucker, *Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads* (Mar. 9, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852260 (finding that because younger women are an expensive demographic to show ads to, "An algorithm which simply optimizes cost-effectiveness in ad delivery will deliver ads that were intended to be gender-neutral in an apparently discriminatory way, due to crowding out."); Latanya Sweeney, *Discrimination in Online Ad Delivery*, Communications of the ACM, May 2013, at 44, https://cacm.acm.org/magazines/2013/5/163753-discrimination-in-online-ad-delivery/.

[27] Ali, et al., *Discrimination Through Optimization, supra* note 14.

and force companies to take steps to determine whether their data practices are likely to lead to discriminatory outcomes.[28] Others that would prohibit discriminatory uses of data include the Digital Accountability and Transparency to Advance Privacy Act (DATA Privacy Act) introduced by Senator Cortez Masto and the Privacy Bill of Rights Act.[29] The Algorithmic Accountability Act of 2019 introduced by Senators Wyden and Booker would also force prospective impact assessments.[30] Congress should look to provisions in these bills for guidance on this matter.

Any new privacy legislation should establish standards that attach substantive legal obligations to collection and use of consumers' data, and that protect Americans from discriminatory uses of data.

4. Congress should not encroach on states' innovative regulation

As Congress considers establishing new privacy and data security protections for Americans' private information, it should not step on the toes of states also racing to protect their citizens in the face of rising privacy threats. Americans are asking for *more* protections for their private information, not less. States are responding to that call.

Indeed, a number of state laws play an important role in filling gaps that exist in federal legislation. Many states have expanded the scope of their data security and breach notification laws to extend protections to previously unregulated market sectors and private data—and consumers in those states are benefiting from those existing laws. For example, Connecticut's data security and breach notification statute covers entities operating at multiple nodes of the health care pipeline.[31] California adopted a data security statute—the Student Online Personal Information Protection Act

---

[28] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019).
[29] Digital Accountability and Transparency to Advance Privacy Act (DATA Privacy Act), S. 583, 116th Cong. (2019); Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019).
[30] 116th Cong. (2019); Algorithmic Accountability Act of 2019, S. 1108, H.R. 2231, 116th Cong. (2019).
[31] C.G.S.A. § 38a-999b(a)(2) ("health insurer, health care center or other entity licensed to do health insurance business in this state, pharmacy benefits manager . . . third-party administrator . . . that administers health benefits, and utilization review company.").

(SOPIPA)—that is tailored to online educational platforms.[32] SOPIPA prompted twenty-one other states to adopt student data security laws modeled on California's example.[33] Minnesota adopted a law requiring Internet Service Providers (ISPs) to maintain the security and privacy of consumers' private information.[34] And Texas now requires any nonprofit athletic or sports association to protect sensitive personal information.[35]

Some states have also expanded the types of information that data holders are responsible for protecting from unauthorized access, or for notifying consumers of when breached. For example, ten states have expanded breach notification laws so that companies are now required to notify consumers of unauthorized access to their biometric data—unique measurements of a person's body that can be used to determine a person's identity.[36] This important step recognizes that a biometric identifier such as a fingerprint or iris scan—unlike an alphanumeric password—cannot be changed after it has been compromised. A large number of states also now require companies to notify consumers about breaches of medical or health data—information that can be used in aid of medical identity theft, potentially resulting in fraudulent healthcare charges and even introduction of false information into one's medical record.[37]

---

[32] West's Ann.Cal.Bus. & Prof.Code § 22584(d)(1) (schools must "[i]mplement and maintain reasonable security procedures and practices . . . and protect that information from unauthorized access, destruction, use, modification, or disclosure.").

[33] Rachel Anderson, *Last Year's Education Data Privacy Legislation* Trends, iKeepSafe Blog, Jan. 17, 2018, https://ikeepsafe.org/last-years-education-data-privacy-legislation-trends/.

[34] M.S.A. § 325M.05 (must "take reasonable steps to maintain the security and privacy of a consumer's personally identifiable information.").

[35] V.T.C.A., Bus. & C. § 521.052 ("implement and maintain reasonable procedures . . . to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.").

[36] States that have done this include Delaware, Illinois, Iowa, Maryland, Nebraska, New Mexico, North Carolina, Oregon, Wisconsin, and Wyoming.

[37] *See* Joshua Cohen, *Medical Identity Theft—The Crime that Can Kill You*, MLMIC Dateline (Spring 2015), *available at* https://www.mlmic.com/wp-content/uploads/2014/04/Dateline-SE_Spring15.pdf ("A patient receiving medical care fraudulently can lead to the real patient receiving the wrong blood type, prescription, or even being misdiagnosed at a later time."). Medical or health data is covered by breach notification laws in Alabama,

And states are doing other important work on privacy as well. In addition to the California Consumer Privacy Act,[38] California also has a law requiring notification about breaches of information collected through an automated license plate recognition system.[39] Vermont has the Data Broker Act.[40] Illinois has the Biometric Information Protection Act.[41] Earlier this year, Maine enacted a new broadband privacy law.[42]

To avoid doing harm to consumers benefiting from these existing consumer protections, any federal legislation on privacy or data security must preserve strong state standards, as well as states' ability to continue innovating on privacy. There are bills currently before the Committee that can be used as a model for crafting this provision. A number of privacy bills before this Committee are silent on preemption of state laws and presumably would only invalidate those that are in conflict. Bills that would expressly avoid preemption of stronger state laws include the Algorithmic Accountability Act and COPRA.[43] In contrast, bills that would explicitly preempt state laws—even those that offer consumers stronger privacy protections and potentially even general consumer protection laws—include the the Balancing the Rights Of Web Surfers Equally and Responsibly Act of 2019 (BROWSER Act) introduced by Senator Blackburn and the U.S. Consumer Data Privacy Act.[44]

Arkansas, California, Delaware, Florida, Illinois, Kentucky, Maryland, Montana, Nevada, North Dakota, Oregon, Puerto Rico, Nevada, Rhode Island, Texas, Virginia, and Wyoming.

[38] California Consumer Privacy Act, https://www.caprivacy.org/ (last visited October 7, 2018).

[39] West's Ann.Cal.Civ.Code § 1798.82(h)

[40] Devin Coldewey, *Vermont Passes First Law to Crack Down on Data Brokers*, TechCruch, May 27, 2018, https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers/.

[41] 740 ILCS 14/1 *et seq.*

[42] Inside Privacy, *Maine Enacts Broadband Privacy Law*, June 28, 2019, https://www.insideprivacy.com/united-states/state-legislatures/maine-enacts-broadband-privacy-law/.

[43] Algorithmic Accountability Act of 2019, S. 1108, H.R. 2231, 116th Cong. (2019); Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019).

[44] Balancing the Rights of Web Surfers Equally and Responsibly Act of 2019, S. 1116, 116th Cong. (2019) (as introduced by S. Blackburn to the S. Comm. on Commerce, Sci., and Transp.); U.S. Consumer Data Privacy Act of 2019, *available at* https://aboutblaw.com/NaZ (discussion draft circulated by S. Wicker in Nov. 2019).

5. There are valuable provisions in multiple bills before this committee

The public interest community has asked for a number of major reforms to set things right. Proposals before this committee contain provisions that would deliver many of those reforms, and the Committee can use those provisions as models to develop legislation that honors the Public Interest Privacy Legislation Principles.[45] For example, provisions in legislation before this Committee would establish a number of the items outlined in those Principles:

- **Consumer rights to data access, quality, portability, and security.** Bills that would give consumers important rights to data access, quality, portability, and security include COPRA and the Privacy Bill of Rights Act, as well as the U.S. Consumer Data Privacy Act discussion draft circulated last week by Senator Wicker.[46]

- **Data minimization.** The Privacy Bill of Rights Act should serve as a model on this point, because it would prohibit the collection of personal information unless it is needed to perform a contract, to provide a requested product or service, or to take steps at the request of the individual.[47] COPRA would prohibit the collection and retention of personal information not covered by the covered entity's articulated purposes as expressed in a privacy policy.[48]

- **A prohibition on discriminatory uses of data.**[49] Congress should look to COPRA as a model on this point, because it prohibits discriminatory uses of data, and also would force companies to take steps to determine whether their data practices are likely to lead to discriminatory

---

[45] *See* Public Interest Privacy Legislation Principles, https://newamericadotorg.s3.amazonaws.com/documents/Public_Interest_Privacy_Principles.pdf.
[46] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019); Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019); U.S. Consumer Data Privacy Act of 2019, *available at* https://aboutblaw.com/NaZ (discussion draft circulated by S. Wicker in Nov. 2019).
[47] Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019) (as introduced by S. Markey).
[48] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019).
[49] *See* discussion *supra* at Section 3, p. 7.

outcomes.[50] Other bills that would prohibit discriminatory uses of data include the DATA Privacy Act and the Privacy Bill of Rights Act.[51] The Algorithmic Accountability Act also provides another example of how companies could be made to detect discriminatory outcomes resulting from their practices.[52]

- **Robust rulemaking authority for a federal agency.** Bills that would establish robust rulemaking authority for a federal agency include COPRA, the Privacy Bill of Rights Act, and the DATA Privacy Act, and these bills can be used as models for crafting agency rulemaking authority.[53] Some bills would only grant much more limited rulemaking authority. For example, the U.S. Consumer Data Privacy Act discussion draft would only give the FTC rulemaking authority to establish requirements for covered entities to verify requests associated with privacy rights, but not to honor those rights more broadly.[54] Other bills would grant rulemaking authority limited to a narrower scope of privacy coverage, such as the Commercial Facial Recognition Privacy Act of 2019 introduced by Senators Blunt and Schatz, the Deceptive Experiences To Online Users Reduction Act (DETOUR Act) introduced by Senators Warner and Fischer, the Algorithmic Accountability Act of 2019, the Do Not Track Act introduced by Senator Hawley, the Data Broker List Act of 2019 introduced by Senators Peters and McSally, and the Protecting Privacy in Our Homes Act introduced by Senator Gardner.[55]

---

[50] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019).
[51] Digital Accountability and Transparency to Advance Privacy Act (DATA Privacy Act), S. 583, 116th Cong. (2019); Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019) (as introduced by S. Markey).
[52] Algorithmic Accountability Act of 2019, S. 1108, H.R. 2231, 116th Cong. (2019).
[53] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019); Digital Accountability and Transparency to Advance Privacy Act (DATA Privacy Act), S. 583, 116th Cong. (2019); Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019) (as introduced by S. Markey).
[54] U.S. Consumer Data Privacy Act of 2019, *available at* https://aboutblaw.com/NaZ (discussion draft circulated by S. Wicker in Nov. 2019).
[55] Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019); Deceptive Experiences to Online Users Reduction Act, S. 1084, 116th

- **Additional staff and resources for an expert agency.** COPRA should serve as a model to grant staff and resources for an expert agency, because it would enable the Federal Trade Commission to form a new privacy and data security bureau, and authorization appropriations for the Commission to carry out all activities associated with the law.[56] The DATA Privacy Act would enable the Commission to appoint additional personnel and authorize appropriations for that purpose.[57] The U.S. Consumer Data Privacy Act would authorization appropriations to assist the Commission with enforcement, but not rulemaking or oversight.[58] The Markey-Hawley bill updating the Children's Online Privacy Protection Act would add a Youth Privacy and Marketing Division to the Federal Trade Commission.[59]

- **Enforcement rights not only at the federal level, but also for state attorneys general and private citizens.** COPRA should serve as a model on enforcement. It would enable individuals to vindicate their own rights in court, and importantly also clearly provides guidelines for meaningful relief.[60] The Privacy Bill of Rights Act also contains language that crafts a private right of action.[61] Most privacy bills currently before this Committee also include critical enforcement powers for state attorneys general. Those that do not include the

---

Cong. (2019); Algorithmic Accountability Act of 2019, H.R. 2231, S. 1108, 116th Cong. (2019); Do Not Track Act, S. 1578, 116th Cong. (2019); Data Broker List Act of 2019, S. 2342, 116th Cong. (2019); Protecting Privacy in Our Homes Act, S. 2532, 116th Cong. (2019).

[56] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019).

[57] Digital Accountability and Transparency to Advance Privacy Act (DATA Privacy Act), S. 583, 116th Cong. (2019).

[58] U.S. Consumer Data Privacy Act of 2019, *available at* https://aboutblaw.com/NaZ (discussion draft circulated by S. Wicker in Nov. 2019).

[59] A bill to Amend the Children's Online Privacy Protection Act of 1998 to Strengthen Protections Relating to the Online Collection, Use, and Disclosure of Personal Information of Children and Minors, and for Other Purposes, S. 748, 116th Cong. (2019).

[60] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019).

[61] Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019) (as introduced by S. Markey).

DETOUR Act, the BROWSER Act, the Data Broker List Act of 2019, and the Protecting Privacy in Our Homes Act.[62]

- **A prohibition on forced arbitration.** Congress should look to COPRA and the Privacy Bill of Rights Act for language prohibiting privacy-related forced arbitration.

A number of proposals also contain other substantial reform measures. For example, COPRA would expressly protect privacy whistleblowers from retaliation for providing information to enforcers.[63] The Do Not Track Act introduced by Senator Hawley would institute a Do Not Track system and require operators of sites and services to honor Do Not Track signals by refraining from data collection.[64] The Data Broker List Act would facilitate enrollment of data brokers in a national registry and place certain restrictions on data brokers.[65] And the Markey-Hawley children's privacy bill would strengthen privacy protections for children and minors.[66]

6. If Congress cannot agree on legislation that embodies the Public Interest Privacy Legislation Principles, perhaps it should not act

One option before Congress is to hold its pen. Although there are many valuable provisions in bills before this Committee that Congress can draw from as it continues to work toward comprehensive consumer privacy legislation, Congress has yet to produce a bipartisan bill that embodies the Public Interest Privacy Legislation Principles advanced by 34 public interest organizations over a year ago and attached here.[67] It is better for Congress to

---

[62] Deceptive Experiences to Online Users Reduction Act, S. 1084, 116th Cong. (2019); Balancing the Rights of Web Surfers Equally and Responsibly Act of 2019, S. 1116, 116th Cong. (2019); Data Broker List Act of 2019, S. 2342, 116th Cong. (2019); Protecting Privacy in Our Homes Act, S. 2532, 116th Cong. (2019).
[63] Consumer Online Privacy Rights Act (COPRA), 116th Cong. (2019).
[64] Do Not Track Act, S. 1578, 116th Cong. (2019).
[65] Data Broker List Act of 2019, S. 2342, 116th Cong. (2019).
[66] A bill to Amend the Children's Online Privacy Protection Act of 1998 to Strengthen Protections Relating to the Online Collection, Use, and Disclosure of Personal Information of Children and Minors, and for Other Purposes, S. 748, 116th Cong. (2019).
[67] *See* Public Interest Privacy Legislation Principles, https://newamericadotorg.s3.amazonaws.com/documents/Public_Interest_Privacy_Principles.pdf.

wait—and allow the states to continue to fill the gap—than to rush to pass something that does not fulfill these important principles.

7. Conclusion

I am grateful for the Committee's attention to these important issues, and for the opportunity to present this testimony. I look forward to your questions.

Public Interest Privacy Legislation Principles

Unregulated data collection and use in the United States has eroded public trust in companies to safeguard and use data responsibly. Surveys show that, while individuals often try to remove or mask their digital footprints,[1] people think they lack control over their data,[2] want government to do more to protect them,[3] and distrust social media platforms.[4]

The current U.S. data privacy regime, premised largely upon voluntary industry self-regulation, is a failure. Irresponsible data practices lead to a broad range of harms, including discrimination in employment, health care, and advertising, data breaches, and loss of individuals' control over personal information. Existing enforcement mechanisms fail to hold data processors accountable and provide little-to-no relief for privacy violations.

The public needs and deserves strong and comprehensive federal legislation to protect their privacy and afford meaningful redress. Privacy legislation is essential to ensure basic fairness, prevent discrimination, advance equal opportunity, protect free expression, and facilitate trust between the public and companies that collect their personal data. Legislation should reflect at least the following ideas and principles:

1. Privacy protections must be strong, meaningful, and comprehensive

Privacy concerns cannot be fully addressed by protecting only certain classes of personal data held by some companies. Legislation should mandate fairness in all personal data processing, respect individuals' expectations for how data should be treated, provide for data portability, and include safeguards against misuse of data, including de-identified and aggregate data. Legislation should advance fundamental privacy rights and require all entities that collect, store, use, generate, share, or sell (collectively, "process") data both online and offline to comply with Fair Information Practices[5] (collection limitation, data

---

[1] *The State of Privacy in Post-Snowden America*, Pew (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america.
[2] Bree Fowler, *Americans Want More Say in the Privacy of Personal Data*, Consumer Reports (May 18, 2017), https://www.consumerreports.org/privacy/americans-want-more-say-in-privacy-of-personal-data.
[3] Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, Pew (Mar. 27, 2018), http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns.
[4] *Id.*
[5] Fair Information Practices are similar to those adopted by the OECD. *See* OECD Privacy Framework, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

quality, purpose specification, use limitation, security safeguards, openness, access and correction rights, and accountability) across the complete life cycle of the data. Legislation should require all data processing to be clearly and accurately explained, justified, and authorized by the individual. People should have the right to know when their data has been compromised or otherwise breached. Additionally, legislation should require entities processing data to adopt technical and organizational measures to meet these obligations, including risk assessments of high-risk data processing.

2. Data practices must protect civil rights, prevent unlawful discrimination, and advance equal opportunity

Legislation should ensure fundamental fairness of and transparency regarding automated decision-making. Automated decision-making, including in areas such as housing, employment, health, education, and lending, must be judged by its possible and actual impact on real people, must operate fairly for all communities, and must protect the interests of the disadvantaged and classes protected under anti-discrimination laws. Legislation must ensure that regulators are empowered to prevent or stop harmful action, require appropriate algorithmic accountability, and create avenues for individuals to access information necessary to prove claims of discrimination. Legislation must further prevent processing of data to discriminate unfairly against marginalized populations (including women, people of color, the formerly incarcerated, immigrants, religious minorities, the LGBTQIA/+ communities, the elderly, people with disabilities, low-income individuals, and young people) or to target marginalized populations for such activities as manipulative or predatory marketing practices. Anti-discrimination provisions, however, must allow actors to further equal opportunity in housing, education, and employment by targeting underrepresented populations where consistent with civil rights laws. Moreover, decades of civil rights law have promoted equal opportunity in brick-and-mortar commerce; legislation must protect equal opportunity in online commerce as well.

3. Governments at all levels should play a role in protecting and enforcing privacy rights

The public consistently call for government to do more, not less, to protect them from misuse of their data. Legislation should reflect that expectation by providing for robust agency oversight, including enhanced rulemaking authority, commensurate staff and resources, and improved enforcement tools. Moreover, no single agency should be expected to police all data processors; therefore, legislation should empower state attorneys general and private citizens to pursue legal remedies, should prohibit forced arbitration, and importantly, should not preempt states or localities from passing laws that establish stronger protections that do not disadvantage marginalized communities.

4. Legislation should provide redress for privacy violations

Individuals are harmed when their private data is used or shared in unknown, unexpected, and impermissible ways. Privacy violations can lead to clear and provable financial injury, but even when they do not, they may, for example, cause emotional or reputational harm; limit awareness of and access to opportunities; increase the risk of suffering future harms; exacerbate informational disparities and lead to unfair price discrimination; or contribute to the erosion of trust and freedom of expression in society. In recognition of the many ways in which privacy violations are and can be harmful, legislation should avoid requiring a showing of a monetary loss or other tangible harm and should make clear that the invasion of privacy itself is a concrete and individualized injury. Further, it should require companies to notify users in a timely fashion of data breaches and should make whole people whose data is compromised or breached.

Signed,

Access Humboldt
Access Now
Berkeley Media Studies Group
Campaign for a Commercial-Free Childhood
Center for Democracy & Technology
Center for Digital Democracy
Center for Media Justice
Center on Privacy & Technology at Georgetown Law
Color of Change
Common Cause
Common Sense Kids Action
Consumer Action
Consumer Federation of America
Consumers Union
Customer Commons
Demand Progress
Free Press Action Fund
Human Rights Watch
Lawyers' Committee for Civil Rights Under Law
Media Alliance
Media Mobilizing Project
National Association of Consumer Advocates
National Consumer Law Center
National Consumers League
National Digital Inclusion Alliance
National Hispanic Media Coalition
New America's Open Technology Institute
Oakland Privacy
Open MIC (Open Media and Information Companies Initiative)
Privacy Rights Clearinghouse
Public Citizen
Public Knowledge
U.S. PIRG
United Church of Christ, OC Inc.