Questions for the Record
Michelle Richardson
Director, Privacy and Data Project
Center for Democracy and Technology

U.S. Senate Committee on the Judiciary

GDPR & CCPA: Opt-ins, Consumer Control, and
the Impact on Competition and Innovation
March 12, 2019

Chairman Graham

1. What are the specific areas of the CCPA that could have a negative impact on competition and innovation? What areas of the CCPA need more clarity, improvement, or removal?

While the California Consumer Privacy Act (CCPA) has dominated conversations about commercial data privacy laws in the United States in recent months, it is too soon to know the full impact of the law. Thus, even as some attempt to measure the purported compliance costs of the CCPA, it is impossible to identify whether -- or if -- the CCPA will have negative impacts on competition or innovation. Companies such as U.S.-focused advertisers and the offline data ecosystem that have been able to ignore EU and other global data protection trends will likely be forced to step up their privacy protections as a result of the CCPA.[1]

CDT has previously suggested several areas where the CCPA could be clarified or improved, including clarifying the definition of personal information and the right of access.[2] The CCPA

[1] *See* Joseph Jerome, *California Privacy Law Shows Data Protection on the March*, ABA Antitrust, Vol. 33:1 (2018).
[2] *See* Ctr. for Democracy & Tech., *A New Day for Privacy Dawns in California (*July 3, 2018), https://cdt.org/blog/a-new-day-for-privacy-dawns-in-california/ (highlighting four areas of the CCPA warranting additional consideration); Future of Privacy Forum, *CCPA, face to face with the GDPR: An in*

does not go into effect until next year, and both legislative and regulatory tweaks to the law are likely. Since its passage in June 2018, the CCPA has already undergone one round of legislative amendments, including a delay of enforcement by the California Attorney General until July 1, 2020.[3] Further, we would reiterate that to the extent that companies claim to support a federal law that would be "stronger" than California's, most of the publicly available industry proposals do not match what is being discussed at the state level.[4]

Ultimately, a federal privacy law that provides clear rules for the collection, use, and disclosure of information, and does not rely on notice and consent, will provide a level playing field and straightforward compliance environment for companies. In this way, it is possible for a federal law to be more impactful than the CCPA, even it is uses different mechanisms.

Senator Grassley - Questions for the Second Panel

1. Please briefly explain the importance of transparency and ensuring that consumers can make informed decisions about the information they share.

Transparency is a foundational privacy principle.[5] Consumers deserve information about how their information is collected, used, shared, and protected, and transparency mandates are important components of both the CCPA and the EU GDPR. However, any privacy framework that rests primarily on transparency will not adequately protect individuals' privacy nor will it restore Americans' trust that companies are responsible stewards of data.

Transparency alone is insufficient for several reasons. First, mandates that companies provide consumers with privacy policies that are both in plain-language and sufficiently detailed to provide meaningful information are competing priorities. Many privacy laws, including the CCPA and GDPR, have required longer privacy policies,[6] but these disclosures are often vague and legalistic.[7] The alternative are simpler "model" disclosures that may be easier for individuals to read but provide little concrete information about what companies are doing with data.[8]

---

depth comparative analysis (Nov. 28, 2018), https://fpf.org/2018/11/28/fpf-and-dataguidance-comparison-guide-gdpr-vs-ccpa/.

[3] *See* S.B. 1121, 2017-18 Leg. (Ca. 2018).

[4] Omer Tene, Twitter (Mar. 7, 2019), https://twitter.com/omertene/status/1103698390452457472.

[5] *See, e.g.*, Robert Gellman, Fair Information Practices: A Basic History, v. 2.18 (Apr. 10, 2017), https://bobgellman.com/rg-docs/rg-FIPshistory.pdf; Fed. Trade Comm'n, Privacy Online: Report to Congress 7 (1998).

[6] Joanna Stern, *Those Privacy Policies Flooding Your Inbox? Print Them Out and They Span a Football Field*, Wall Street J. (May 17, 2018), https://www.wsj.com/articles/privacy-policies-flooding-your-inbox-how-to-cut-through-the-gibberish-1526565342.

[7] The FTC acknowledged as such in 2010. *See* Press Release, Fed. Trade Comm'n, FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers (Dec. 1, 2010), https://www.ftc.gov/news-events/press-releases/2010/12/ftc-staff-issues-privacy-report-offers-framework-consumers. There is a rich history of academic literature on the failure of the privacy policy, e.g., Fred Cate, *The Limits of Notice and Choice*, 8 IEEE SEC. & PRIVACY 59, 59–62 (2010), and commentators

Second, even if individuals wanted to review how companies handle their data, it would require upwards of 76 work days per year to read every privacy policy an average American comes across each year.[9] Even well-informed and privacy-minded individuals cannot self-manage their privacy,[10] and most Americans also operate under fundamentally incorrect assumptions about how their privacy is protected.[11]

Third and finally, even if individuals could make truly informed decisions about how to share data, they need only make one mistaken decision or have a pressing need or desire to lose complete control over their information. For example, expectant mothers who intend to protect the privacy of their pregnancies face a near impossible task if they wish to use a single pregnancy or fertility app or make any purchases to prepare for their newborn.[12] In the words of one researcher, the efforts to main control over what one woman viewed as intensely private information made her "look like a criminal."[13] More transparency will not address this challenge, and unfairly burdens individuals with the impossible task of protecting their privacy.

2. Often times, comprehensive regulations end up just benefiting the large, entrenched entities that have teams of lawyers to ensure compliance. Should small businesses be treated differently in any federal data privacy framework? And if so, how?

CDT believes that a strong privacy law can establish clear ground rules that level the playing field for businesses large and small while protecting individuals from unfair, surprising, and privacy-invading practices. This can be done without exempting smaller businesses from a privacy regime altogether, which we understand is being proposed by a number of stakeholders.

Certain brightline rules --like purpose limitations--can ensure that startups and small businesses understand what is required of them while preventing established entities from capitalizing on

---

continue to criticize the structure of privacy policies from both angles, e.g., Priya Kumar, *Privacy Policies and Their Lack of Clear Disclosure Regarding the Life Cycle of User Information* (2016), *available at* https://rankingdigitalrights.org/2017/01/06/companies-fail-privacy-policies/; Natasha Lomas & Romain Dillet, *Terms And Conditions Are The Biggest Lie Of Our Industry*, TechCrunch (Aug. 21, 2015), https://techcrunch.com/2015/08/21/agree-to-disagree/.

[8] *See* Ctr. for Democracy & Tech., Letter to U.S. Senate on Improving Data Privacy, Protection and Collection Practices in Financial Data (Mar. 15, 2019), https://cdt.org/insight/letter-to-us-senate-on-improving-data-privacy-protection-and-collection-practices-in-financial-data/ (highlighting limitations of GLBA Model Privacy Notices).

[9] *See, e.g.*, Alicia McDonald and Lorrie Cranor, *The Cost of Reading Privacy Policies*, J. of Law and Pol. for the Information Society (2008) (estimating that it would take an average 244 hours per year for each individual to read the privacy policies of each web site visited once a month for a total cost of $3,534 a year).

[10] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013)

[11] Joseph Turow, *Let's Retire the Phrase 'Privacy Policy'*, N.Y. Times (Aug. 20, 2018), https://www.nytimes.com/2018/08/20/opinion/20Turow.html.

[12] Kashmir Hill, *What Happens When You Tell the Internet You're Pregnant*, GIZMODO (July 27, 2017), https://jezebel.com/what-happens-when-you-tell-the-internet-youre-pregnant-1794398989.

[13] Janet Vertesi, Opinion, *My Experiment Opting Out of Big Data Made Me Look Like a Criminal,* TIME (Apr. 30, 2014), http://time.com/83200/privacy-internet-big-data-opt-out/.

the access they have to the internet ecosystem. For example, our federal legislative proposal would place limits on how all companies can collect and use sensitive data like biometrics and geolocation when it is not necessary to the operation of a product or service that a user requests. As Engine Advocacy, a trade association representing the startup ecosystem, explained to the Senate Commerce Committee, a mapping app may require geolocation data, but a flashlight app has no need to access a user's geolocation to deliver that service to a consumer.[14] Such a limitation can be understood by lay readers, and would not reward the practices of large entities shuffling personal information amongst the many different products they offer.

Other commonly discussed components are core to individual rights and do not necessarily need require technical sophistication to implement. This includes the rights to know, access, and delete information, for example.

We also note that too much flexibility just leads to uncertainty, and that is certainly borne more heavily by small actors. Congress should avoid relying solely or primarily on corporate accountability mechanisms, including risk assessments, formal privacy programs, and other documentation requirements, that will create compliance costs. Instructing companies to engage in risk assessments rather than simply prohibiting risky practices creates requirements that are easier for larger entities to throw teams of lawyers at.[15]

Much has been made of the "hundreds of years of human time" spent by some of the largest technology companies in the world to prepare for the GDPR,[16] but data-driven businesses that collect and traffic in personal information should be burdened by privacy laws. This extends to small businesses that are engaged in practices that impinge on privacy. We reiterate that Cambridge Analytica had fewer than 250 employees;[17] Exactis, a data broker that leaked the personal information of 150 million Americans, had less than 10 employees.[18]

3. If Congress enacts federal data privacy legislation, how do we ensure that companies are still incentivized to innovate in their privacy and data protections, rather than just 'check the box' of regulatory compliance?

---

[14] Testimony of Evan Engstrom, Executive Director, Engine Advocacy and Research Foundation Before the Senate Commerce Committee (Mar. 26, 2019), *available at* https://www.commerce.senate.gov/public/_cache/files/949f1fc8-dc28-4760-9f47-6cb925a1549e/0AE3566F5899E50A6C4D08C7142D8752.testimony-of-evan-engstrom-engine.pdf.

[15] Ctr. for Democracy & Tech., *The Washington Privacy Act Raises Important Considerations for Comprehensive Privacy Proposals* (Feb. 7, 2019), https://cdt.org/blog/the-washington-privacy-act-raises-important-considerations-for-comprehensive-privacy-proposals/.

[16] Ashley Rodriguez, *Google says it spent "hundreds of years of human time" complying with Europe's privacy rules*, Quartz (Sept. 26, 2018), https://qz.com/1403080/google-spent-hundreds-of-years-of-human-time-complying-with-gdpr/.

[17] Cambridge Analytica, Crunchbase, https://www.crunchbase.com/organization/cambridge-analytica#section-overview (last visited Apr. 1, 2019).

[18] Kari Paul, *What is Exactis—and how could it have leaked the data of nearly every American?*, MarketWatch (June 29, 2018), https://www.marketwatch.com/story/what-is-exactisand-how-could-it-have-the-data-of-nearly-every-american-2018-06-28.

At present, negative headlines and the off-chance enforcement action are the primary incentives to encourage companies to innovate in their privacy and data protections. This status quo has neither served consumers nor provided any generalized standard of privacy protection expected of businesses. Federal data privacy legislation has the opportunity to set a baseline set of protections and expectations for how data is to be handled.

As discussed below, we believe a federal data privacy law should establish clear ground rules that clarify the contours of what individual rights and expectations to data should be as well as clear prohibitions against specific unfair, surprising, and privacy-invading practices. Actionable user rights and clear and simple limits on data processing minimizes compliance exercises by avoiding subjectivity and uncertainty.

4. How do we best craft a federal data privacy law that keeps pace with our ever-evolving tech and data landscape? And can we do that without giving unfettered discretion to the regulators?

A federal data privacy law should establish clear ground rules that clarify the contours of what individual's rights and expectations to data should be as well as clear prohibitions against specific unfair, surprising, and privacy-invading practices. CDT recommends that Congress generally prohibit the following data processing practices, subject to several clearly scoped exceptions, when processing is not required to provide or add to the functionality of a service or feature that the user has affirmatively requested: (1) The processing of biometric information to identify a person; (2) The processing of un-anonymized precise geospatial information; (3) The processing of health information; (4) The use of children's information for targeted advertising and disclosure to third parties; (5) The licensing or sale to third parties of the contents of communications or the parties to a communication (such as call or email logs); (6) The retention, use, or disclosure of audio and visual recordings; and (7) The use of probabilistic inferences to tracking people across different devices. An explicit statement of congressional intent can provide direction to advocacy organization, companies, and regulators in order to ensure a privacy law's intentions keep up with evolving technology.

There must also be mechanisms put in place to assess and evaluate the state of federal privacy protections over time. CDT recommends regular reporting by an entity, such as the Government Accountability Office, to assess how best to update and improve existing privacy laws and to identify any inconsistencies with a baseline comprehensive privacy framework.

Senator Sasse - Questions for Panel II

1. Aside from situations in which compliance costs lead to higher product prices and foregone spending on research and development, in what ways is CCPA affecting Americans outside of California?

While the California Consumer Privacy Act (CCPA) has dominated conversations about commercial data privacy laws in the United States in recent months, the reality is that it is too soon to know the full impact of the law. The CCPA does not go into effect until next year, and both legislative and regulatory tweaks to the law are likely. Since its passage in June 2018, the CCPA has already undergone one round of legislative amendments, including a delay of enforcement by the California Attorney General until July 1, 2020.[19]

The CCPA has encouraged state legislators and attorneys general across the country to advocate for stronger privacy laws in their own states. Since the CCPA's passage, state lawmakers in Vermont have put in place a data broker registry and other states are advancing comprehensive privacy proposals, as well as targeted efforts to address privacy issues involving broadband, geolocation data, and biometrics.

2. Which types of sites, apps, and platforms are able to provide different user experiences between California and the rest of the country in a manner that is technologically feasible and cost-effective? Which are not?

It is not yet clear whether covered entities will try to limit CCPA rights to Californians or extend them to all users regardless of location. In the event certain sites, apps, or platforms either decide to block California residents or to offer an alternative user experience, geofencing technologies make both options technically feasible and not cost prohibitive. If the GDPR serves as a guide, we would further anticipate that the California Attorney General will provide specific guidance to small businesses and startups.

3. What is a principles way we can think about the possibility of federal preemption in the data privacy context? When is not appropriate to let states regulate as they wish, even if we disagree with their policy choices? In what situations should we be comfortable with letting one state drive nationwide policy as a practical matter?

Data privacy impacts and touches upon countless different state laws beyond the CCPA. Before it would be appropriate to discuss the possibility of federal preemption, lawmakers must put forward a strong proposal that can be thoroughly vetted by different stakeholders outside of traditional actors in the technology policy community and work to establish a detailed legislative record of its intentions.[20]

While digital commerce may raise national implications with respect to regulation and legal doctrine under the Dormant Commerce Clause, the stakes of poor data privacy and security practices are too high to discourage states from acting on behalf of their citizens in the absence of federal action. The processing and protection of personal information directly impacts state

[19] *See* S.B. 1121, 2017-18 Leg. (Ca. 2018).
[20] Peter Swire, *Federal preemption of state privacy laws and the issues that may arise*, IAPP Privacy Tracker (Jan. 10, 2019), https://iapp.org/news/a/swire-part-2-federal-preemption-of-state-privacy-laws-and-the-issues-that-may-arise/.

residents, and eleven states explicitly recognize a right to privacy in their state constitutions.[21] Despite repeated calls by CDT, industry stakeholders, and prior administration officials, Congress has declined to set comprehensive privacy protections. Unless and until Congress acts, states will be compelled to act and should be encouraged to experiment with different proposals.

4. To what extent has GDPR deprived European users from accessing particular types of content on the internet?

Much has been made of the fact that more than 1,000 U.S. news sites shut down service to European users after May 25, but most of these sites and services are owned by just a few companies that had small amounts of traffic in the EU.[22] Rather than block European readers, *USA Today* instead removed some ad-related software that harvests information and tracks the online behaviors of its readers. This is the complexity of adtech: *USA Today*'s American website is 5.5 megabytes in size and includes more than 800 ad-related requests for information involving 188 different domains.[23] In contrast, the EU-facing site is less than half a megabyte in size and contains no third-party content. This website not only does less surreptitious tracking, but it also benefits from loading faster.

Other publishers have taken more creative approaches. After the GDPR went into effect, *The New York Times* cut off advertising exchanges in Europe and kept growing ad revenue for itself.[24] The paper's Vice President of Advertising Data called privacy laws that reduce reliance on third-party ad targeting a "win-win-win" for publishers, advertisers, and importantly, consumers.[25] Earlier this year, *The Washington Post* committed to "go beyond cookie-based ad targeting and match ads to people without being 'creepy'."[26] The Local Media Consortium currently is exploring consumer-friendly privacy policies and standards for smaller online publishers.[27]

---

[21] National Conference of State Legislatures, Privacy Protections in State Constitutions (Nov. 7, 2018), www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

[22] *GDPR: US news sites unavailable to EU users under new rules*, BBC News (May 25, 2018), https://www.bbc.com/news/world-europe-44248448.

[23] Mathew Ingram, *Four days into GDPR, US publishers are starting to feel the effects*, Columbia Journalism R. (May 29, 2018), https://www.cjr.org/the_new_gatekeepers/gdpr-rules-publishers.php.

[24] Jessica Davies, *After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue*, Digiday (Jan. 16, 2019), https://digiday.com/media/new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/.

[25] Kendell Timmers, *Third-Party Data Is A Bad Habit We Need To Kick*, AdExchanger (Feb. 22, 2019), https://adexchanger.com/the-sell-sider/third-party-data-is-a-bad-habit-we-need-to-kick/.

[26] Lucia Moses, *The Washington Post is trying to go beyond cookie-based ad targeting and match ads to people without being 'creepy'*, Business Insider (Mar. 7, 2019), https://www.businessinsider.com/washington-post-goes-beyond-cookie-based-ad-targeting-with-feedbuilder-2019-3.

[27] Information Trust Exchange, Multi-stakeholder convening process explained: How to develop consumer-friendly privacy policies and standards, *available at* https://infotrust.org/multi-stakeholder-convening-process-to-develop-consumer-friendly-privacy-policies-and-standards/ (last visited Apr. 1, 2019).

It is also important to note that not every withdrawal from the market is a loss for consumers. Some examples of companies allegedly impacted by the GDPR, like the marketing company that peddled "Klout" scores[28] or the online game serving approximately two dozen active players,[29] withdrew from the EU rather than continue moribund businesses.

5. Which aspects of GDPR, CCPA, and proposed aspects of potential federal legislation most worry you in terms of protecting incumbents in particular markets and creating major barriers to entry for new firms?

CDT believes that a strong privacy law can establish clear ground rules that level the playing field for businesses large and small. Both the GDPR and CCPA establish a set of individual rights, including transparency, access, and deletion that any responsible business should be able to provide regardless of size or industry. Companies that collect or use personal information should be obligated to afford individuals some rights to that data.

Bright line rules are more fair to businesses and can be crafted to better comport with consumer expectations. Unfortunately, while the GDPR creates a clear set of individual rights to information that should be emulated in the United States and expanded beyond what is included in the CCPA, the GDPR also requires companies to be accountable for their data practices. While this is a good idea in theory, in practice it may create significant compliance obligations, including risk assessments, formal privacy programs, and other documentation requirements. Instructing companies to engage in risk assessments rather than simply prohibiting risky practices creates requirements that are easier for larger entities to throw teams of lawyers at.[30]

6. Which aspects of GDPR, CCPA, and proposed aspects of potential federal legislation most worry you in terms of harming innovation? How much should we worry about regulation hampering innovation in the West and giving China a competitive advantage in the development of new technology such as artificial intelligence?

Companies, including startups, can adapt to any set of privacy rules that are clear and consistent. The primary challenge of the GDPR and the CCPA is that both frameworks include provisions and requirements that are not clear. Article 25 of the GDPR, for example, mandates that companies deploy state-of-art privacy by design that is tailored to numerous factors, including (1) the cost implementation, (2) the nature and scope of processing, and (3) risks to individuals, among other factors.[31] While this is a good general purpose requirement, the other

---

[28] Garett Sloane, *Out of Klout*, AdAge (May 10, 2018), https://adage.com/article/digital/klout-social-media-scoring-service-shutting/313470.
[29] Owen S. Good, *Super Monday Night Combat will close down, citing EU's new digital privacy law*, Polygon (Apr. 28, 2018), https://www.polygon.com/2018/4/28/17295498/super-monday-night-combat-shutting-down-gdpr.
[30] Ctr. for Democracy & Tech., *The Washington Privacy Act Raises Important Considerations for Comprehensive Privacy Proposals* (Feb. 7, 2019), https://cdt.org/blog/the-washington-privacy-act-raises-important-considerations-for-comprehensive-privacy-proposals/.
[31] EU General Data Protection Regulation Art. 25.

accountability provisions in the GDPR ensure that companies need to document and record much of these processes, which remain subject to regulatory enforcement action. The CCPA, on the other hand, includes confusing and overlapping definitions of personal information and de-identified, pseudonymized, and aggregate data. The absence of clear rules and clear prohibitions can harm innovation by making it unclear what business practices are and are not out of bounds.

Increasingly, longstanding privacy principles that call on companies to (1) minimize data collection and (2) specify the purposes for which they process data have been criticized as being in tension with developments in artificial intelligence. Such claims belie the fact that companies today have access to tremendous amounts of data, and privacy regulations seek only to place guardrails around the unlimited and unrestricted collection and use of data. Even entities like Google, which are at the vanguard of developments in machine learning, have acknowledged the need to "[p]lace reasonable limitations on the manner and means of collecting, using, and disclosing personal information."[32]

Further, developments in new technologies should not come at the expense of Americans' privacy interests. Advances in location tracking,[33] biometric tracking and analysis,[34] and social scoring in China[35] have been deployed in a fashion that would antithetical to our democratic society. Congress legislating in these areas is a way to ensures that the digital dignity of Americans is protected.[36]

7. In terms of the different proposals for giving the Federal Trade Commission new rulemaking authority, how should we think about balancing between ensuring flexibility to adapt a regulatory framework to fit emerging technologies and avoiding delegation of what should be lawmaking authority properly exercised by Congress to a "fourth branch" of government?

Most importantly, Congress should take it upon itself to (1) establish clear ground rules that clarify the contours of what individual's rights and expectations to data should be, and (2) enact clear prohibitions against specific unfair, surprising, and privacy-invading practices. Such clarity written into statute can help keep FTC rulemaking to a predetermined set of issues.

---

[32] Keith Enright, *Proposing a framework for data protection legislation*, Google Public Policy (Sept. 24, 2018), https://www.blog.google/outreach-initiatives/public-policy/proposing-framework-data-protection-legislation/.
[33] Uptin Saiidi, *Retailers can track your movements inside their stores. Here's how*, CNBC (Mar. 7, 2019), https://www.cnbc.com/2019/03/08/how-retailers-can-track-your-movements-inside-their-stores.html.
[34] Xue Yujie, *Camera Above the Classroom*, Sixth Tone (Mar. 26, 2019), https://www.sixthtone.com/news/1003759/camera-above-the-classroom.
[35] Shannon Liao, *China banned millions of people with poor social credit from transportation in 2018*, Verge (Mar. 1, 2019), https://www.theverge.com/2019/3/1/18246297/china-transportation-people-banned-poor-social-credit-planes-trains-2018.
[36] Rob Lever, *Facebook's call for global internet regulation sparks debate*, Phys.Org (Apr. 1, 2019), https://phys.org/news/2019-04-facebook-global-internet-debate.html.

To be clear, Congress can write a statute, and the FTC can write rules, that govern data by their nature or use instead of the technology used to create the data. For example, protecting precise geolocation information need not peg those protections to any particular type of device or application.

8. Do you foresee any situations in which data portability requirements actually enhance some firms' abilities to build more data-rich profiles of individual users?

CDT believes that individuals should have the right to access and port their information, where technically feasible. Absent that, individuals should be given the ability to download their information. This is essential to avoid lock-in and having personal information be trapped within the ecosystem of a certain firm.

However, if implemented incorrectly, portability requirements pose several serious risks to the privacy, security, and integrity of information. Parties to a portability transaction must have strong security controls in place, including encryption of data in transit, and data stewardship measures to avoid unauthorized third party data access and misuse.[37]

It is true that smaller companies may have fewer capabilities to process portability requests and implement those mechanisms securely[38] and mature companies may be better positioned to offer incentives for users to port data away from new entrants that pose a competitive threat. Our proposal tasks the National Institute for Standards & Technology (NIST) with convening working groups to study these issues.

9. Do you foresee any situations in which opt-in requirements actually increase the amount and types of data that firms collect from individual users?

Opt-in requirements will generally make it harder for companies to collect information from individuals, but companies have become experts at architecting consent flows to ensure individuals provide permission for data collection and use. Rarely do these practices constitute meaningful consent as understand by average Americans. CDT believes Congress ought to put in place guardrails around sensitive data practices where processing is unrelated to a product or service requested by an individual.

10. To what extent do you think privacy policies and user agreements are drafted deliberately to dissuade users from closely reading them?

[37] Data Transfer Project Overview and Fundamentals 3 (July 20, 2018), *available at* https://datatransferproject.dev/dtp-overview.pdf.
[38] Sen. Mark Warner, Potential Policy Proposals for Regulation of Technology Firms -- Draft (Jul 2018), *available at* https://regmedia.co.uk/2018/07/30/warner_social_media_proposal.pdf.

Transparency is a foundational privacy principle,[39] but well-meaning calls for more transparency have created a digital ecosystem governed by public privacy policies. As data collection and use becomes more aggressive, this initial emphasis on transparency has led to a greater focus on increased disclosure as a response. While Americans often believe privacy policies are designed to protect them,[40] the reality is that these disclosures are designed and drafted to meet legal compliance obligations.[41] Many privacy laws, including the CCPA and GDPR, have required longer privacy policies,[42] but these disclosures are often vague and legalistic.[43] The alternative are simpler "model" disclosures that may be easier for individuals to read but provide little concrete information about what companies are doing with data.[44]

Mandates that companies provide consumers with privacy policies that are both in plain-language and sufficiently detailed to provide meaningful information are competing priorities, and transparency and other disclosure requirements will often become legal compliance exercises.

Senator Hirono

1. You listed as your first priority for data privacy legislation the ability for an individual to access, correct, delete, and port personal information. We heard testimony that requirements like these are too burdensome on businesses because it is too difficult to confirm that the individual making the request is who they say they are. Is this a valid criticism? Why or why not?

---

[39] *See, e.g.*, Robert Gellman, Fair Information Practices: A Basic History, v. 2.18 (Apr. 10, 2017), https://bobgellman.com/rg-docs/rg-FIPshistory.pdf; Fed. Trade Comm'n, Privacy Online: Report to Congress 7 (1998).

[40] Joseph Turow, *Let's Retire the Phrase 'Privacy Policy'*, N.Y. Times (Aug. 20, 2018), https://www.nytimes.com/2018/08/20/opinion/20Turow.html.

[41] *See, e.g.*, California Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 (2004).

[42] Joanna Stern, *Those Privacy Policies Flooding Your Inbox? Print Them Out and They Span a Football Field*, Wall Street J. (May 17, 2018), https://www.wsj.com/articles/privacy-policies-flooding-your-inbox-how-to-cut-through-the-gibberish-1526565342.

[43] The FTC acknowledged as such in 2010. *See* Press Release, Fed. Trade Comm'n, FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers (Dec. 1, 2010), https://www.ftc.gov/news-events/press-releases/2010/12/ftc-staff-issues-privacy-report-offers-framework-consumers. There is a rich history of academic literature on the failure of the privacy policy, e.g., Fred Cate, *The Limits of Notice and Choice*, 8 IEEE SEC. & PRIVACY 59, 59–62 (2010), and commentators continue to criticize the structure of privacy policies from both angles, e.g., Priya Kumar, *Privacy Policies and Their Lack of Clear Disclosure Regarding the Life Cycle of User Information* (2016), *available at* https://rankingdigitalrights.org/2017/01/06/companies-fail-privacy-policies/; Natasha Lomas & Romain Dillet, *Terms And Conditions Are The Biggest Lie Of Our Industry*, TechCrunch (Aug. 21, 2015), https://techcrunch.com/2015/08/21/agree-to-disagree/.

[44] *See* Ctr. for Democracy & Tech., Letter to U.S. Senate on Improving Data Privacy, Protection and Collection Practices in Financial Data (Mar. 15, 2019), https://cdt.org/insight/letter-to-us-senate-on-improving-data-privacy-protection-and-collection-practices-in-financial-data/ (highlighting limitations of GLBA Model Privacy Notices).

The right to access, correct, delete, and port personal information, with reasonable exceptions, should be basic requirements for companies that collect personal information. Many businesses are already providing these rights under GDPR. Congress can draft these requirements in a way that is reasonable and not overly burdensome for companies to comply with. While it is reasonable for businesses to ask for clarity in these requirements, it is not true that businesses have no way to confirm the identity of the individual making the request. Many businesses already use a range of methods to confirm customers' identity for security, age verification, and other purposes, using various forms of identification, public records, and/or images submitted by the individual. It would also be appropriate for Congress to provide an exception to these rights—as CDT does in its draft privacy legislation— when the individual cannot reasonably document or confirm his or her identity to the covered entity.

2. What lessons can we learn from the GDPR and Europe's implementation of it? Is the GDPR something that should be adopted wholesale in the United States or are there areas it can be improved?

It is still very early days for the GDPR, but we can point to one aspect of the law that should be adopted in the United States and one that could be improved. The individual rights to access, correct, and delete personal information, with some exceptions, should be non-controversial. Entities covered by the GDPR will already have to implement these systems for their EU users, so there is no reason not to expect people in the US to enjoy the same rights. However, the GDPR on its face does not include clear, specific rules and prohibitions with respect to the collection and use of data. We believe a more defined set of rules would provide US companies and customers with the clarity they need to operate with confidence and trust.

In terms of enforcement, European Data Protection Authorities (DPAs) have focused on certain sensitive data types, including geolocation and health data, and failures by companies to adequately inform individuals of their data practices. Large companies have been subject to the most scrutiny, and regulators have signaled a willingness to work with smaller companies to help them become compliant. These early observations suggest that enforcement discretion can help triage privacy concerns and give smaller entities time to get up to speed.

Senator Booker

1. Marginalized communities, and specifically communities of color, face a disproportionate degree of surveillance and privacy abuses. This has been the case since the Lantern Laws in eighteenth-century New York City (requiring African Americans to carry candle lanterns with them if they walked unaccompanied in the city after sunset) up through the stop-and- frisk initiatives of more recent years.

There are echoes of this tradition today in the digital realm as marginalized communities suffer real harm from digital discrimination. For example, in recent years we have seen many instances of housing discrimination and digital redlining, employment discrimination through digital profiling and targeted advertising, exploitation of low tech literacy through misleading

notice and choice practices, discriminatory government surveillance and policing practices, and voter suppression and misinformation targeting African Americans and other minorities.

I am concerned that—rather than eliminating the bias from our society—data collection, machine learning, and data sharing may actually augment many of the kinds of abuses we fought so hard to eliminate in the Civil Rights Movement. We need privacy legislation that is centered around civil rights.

A. In your view, is a private right of action critical to protecting the civil rights of individuals affected by data collection and disclosure practices?

To the extent that existing civil rights laws provide a private right of action, a federal privacy law should not limit those rights. When it comes to enforcing a new overarching data privacy law, CDT has focused on empowering the FTC and state attorneys general to bring enforcement actions on behalf of their constituents. We understand that private rights of action have played important roles in other consumer protection regimes and would be happy to discuss further the scope of such rights.

B. How easy is it for seemingly non-sensitive information like a ZIP Code to become a proxy for protected class or other sensitive information? How can that information be used to discriminate?

Many different attributes, interest categories, or biographical data points can act as proxies for protected classes. ZIP codes are a notable proxy for race and economic status, but even things as seemingly benign as an interest in hiking can be a proxy for race. This means that ad targeting and personalization can have discriminatory outcomes even if neither the advertiser nor the platform has discriminatory intent. If an advertiser does have discriminatory intent, they can use these segments to exclude protected classes from opportunities or to target them with predatory offers or harmful content.

C.. Significant amounts of data about us are gathered by companies most people have never heard of. Do we need a registry of data brokers, similar to what Vermont established last year?

CDT supports increased transparency measures around data brokerage, and our draft legislation would require data brokers to register with the FTC and provide information into their sources of personal information and how people can exercise their rights to access, correct, delete, or port information held by the data broker. It would also require the FTC to create or facilitate the creation of an accessible online mechanism for individuals to identify data brokers.

2. The tech journalist Kashmir Hill recently wrote a widely circulated article on her efforts to leave behind the “big five” tech companies—Facebook, Google, Apple, Microsoft, and Amazon. Using a VPN, she blocked all of the IP addresses associated with each company and then chronicled how her life changed. She experimented first by blocking individual companies, and

then, at the end of the series, she blocked all five at once. Ms. Hill found that—to varying degrees—she could not get away. Repeatedly, her efforts to intentionally block one company created unpredictable ripple effects for engaging with other, seemingly unrelated, companies and services. Ms. Hill's article spoke to how pervasive these companies are and how much data they capture about us when we're not even (knowingly) using their services.1

A. How would you respond to the following argument? "If people are uncomfortable with the data practices of certain tech companies, they simply shouldn't use their services."

Opting out of these services is not a real option. We rely on search, location services, digital payment processors, and countless other data-processing services just to get through an average day. People often do not have a choice, or don't get to choose, between multiple offerors of the same service, either because they don't exist or because an entity (such as a school, employer, social association, service provider, etc.) is forcing them to use a particular service. Even where there are options, it can be very difficult and prohibitively time consuming to compare privacy policies. Industry practices, market forces, and cognitive and temporal limits prevent people from being able to make choices that align with their personal privacy concerns or values. We need a law that shifts the burden of choosing privacy away from individuals and onto the companies that process their information.

B. What does providing consent mean in a world where it's extremely difficult to avoid certain companies?

For the reasons listed in our answer to part A, consent is often an ineffective means of protecting privacy. We need a new paradigm that does not rely on the fiction of notice and consent.

3. It would take each of us an estimated 76 working days to read all the digital privacy policies we agree to in a single year.2 Most people do not have that much time. They might prefer something simple, easy, and clear—something much like the Do-Not-Track option that has been featured in most web browsers for years.

However, there is a consensus that Do-Not-Track has not worked, because despite the involvement and engagement of stakeholders across the industry, only a handful of sites actually respect the request. A 2018 study showed that a quarter of all adult Americans were using Do-Not-Track to protect their own privacy—and yet 77 percent of Americans were unaware that Google, Facebook, and Twitter don't respect Do-Not-Track requests.3 Just last month, Apple removed the feature from its Safari browser because, ironically, Do-Not-Track was being used for browser fingerprinting, i.e., having the feature turned on was used to distinguish individual users and track them across the web.4

A. What purpose does a notice-and-consent regime serve if the most prominent consent mechanism is only regarded as a suggestion at best?

A notice-and-consent regime is ineffective to protect privacy and we should not rely on it in crafting US privacy legislation. Insead, we should have clear rules for data processing and clear prohibitions on unfair and discriminatory data practices.

B. How much faith should the failure of Do-Not-Track give us in the ability of the industry stakeholders to regulate themselves?

Do-Not-Track also demonstrates that voluntary or self-regulatory solutions will never be a wholly effective way to address privacy concerns. Not only do the largest actors not respect Do-Not-Track but also industry was never able to agree on the design and implementation of the standard.

C. In your view, should this approach be abandoned, or would federal legislation requiring companies to respect the Do-Not-Track signal breathe new life into the mechanism?

Requiring companies to respect Do-Not-Track or any other design solution to privacy would be a step forward, though not comprehensive in itself to protect privacy. Consumers should be offered many more rights-e-especially in what happens to data after it *is* collected--including the rights to access, correct, and delete information that is shared with companies, and the right to reasonable security for the data they share. They should also be able to expect that their data will not be used in discriminatory ways or for secondary purposes when the data is especially sensitive.

4. Given that California has enacted its own privacy legislation that will take effect next year, much of the discussion at the hearing centered on how a federal data privacy law will affect state-level efforts to regulate in the same space. However, most of our existing privacy statutes do not include provisions to overrule stricter protections under state law.5 These preemption provisions are the exception rather than the rule, and became more prevalent starting in the 1990s in statutes like the Children's Online Privacy Protection Act of 1998, the CAN-SPAM Act of 2003, and the 1996 and 2003 updates to the Fair Credit Reporting Act.

A. In your view, should a federal data privacy law preempt state data privacy laws? Why?

First, any state preemption is only appropriate if the preempting federal law is strong, meaningful, and comprehensive. It is appropriate for a strong and comprehensive federal privacy regime to preempt state privacy laws to a degree, but preemption must be scoped and drafted very carefully so as not to sweep in protections such as civil rights, anti-stalking, and other laws that may be related but would not be redundant to a federal consumer privacy law.

B In your view, should a federal data privacy law implement the requirements of the California Consumer Privacy Act as a floor? If not, please explain the most significant change you would suggest.

CDT supports a federal privacy law that is stronger than the CCPA, and we believe that means the structure and mechanisms in the law would be significantly different from the CCPA. Ideally, a stronger federal law should preempt a weaker CCPA and protect Californians at the same high standard as all other Americans. For example, CDT's draft legislation would require entities that collect personal data to provide individuals with the names of third parties with whom their personal information is disclosed. We would also advocate for a federal law that does not rely on notice and opt-out to protect privacy but that includes clear and meaningful rules and prohibitions around the collection and use of data.

C. The specific wording of a proposed preemption provision will invite considerable debate in Congress and, ultimately, will still require courts to interpret and clarify the provision's scope. Should the Federal Trade Commission have notice-and-comment rulemaking authority to aid in the statute's interpretation and to clarify which types of state laws are preempted? Or, alternatively, is case-by-case adjudication of multiple state privacy laws preferable? Would rulemaking authority obviate the need for Congress to solve each and every preemption issue in drafting the text?

CDT does not oppose rulemaking authority for the FTC to clarify the scope of preemption, but Congress first needs to do the hard work of drafting the appropriate scope. Congress cannot rely on the FTC to make all of the hard decisions.

D. The preemption language in, for example, the amendments to the Fair Credit Reporting Act was included as part of a heavily negotiated process in which consumers received a package of new rights in exchange for certain preemption provisions.6 Rather than centering the federal privacy bill debate on the existence of a preemption provision, shouldn't our starting point be: "Preemption in exchange for what?" In other words, what basic consumer protections should industry stakeholders be willing to provide in exchange for preemption? Do the requirements of the California Consumer Privacy Act represent a good floor for negotiating preemption?

We agree that the debate should be focused on the substance of a strong and meaningful federal privacy law, not on the existence of preemption. We also believe that we can and should push for a federal law that is stronger than the CCPA. In other words, a federal law that only goes as far as the CCPA would not be strong enough to warrant preempting states from passing stronger laws.

5. At the hearing, several witnesses indicated that opt-out requirements that permit users to tell companies not to process and sell their data are more protective of data privacy and more conducive to the user experience, since they do not impose the "take it or leave it" dynamic that

opt-ins tend to create. In your view, are opt-outs preferable to opt-ins in terms of both data privacy and user experience? Why?

Both opt-ins and opt-outs fail to meaningfully protect privacy because they force the user to assume the untenable burden of evaluating every privacy policy and notice and making choices that align with their best interests. There is no reason that opt-ins would necessarily create a "take it or leave it" dynamic. Companies choose whether their users must agree to their data sharing practices as a condition of using the service, and this decision can be completely independent from the decision about whether to design user controls as opt-ins or opt-outs. Defaults are "sticky," meaning that people tend not to change them, so opt-outs are typically more likely to elicit more permission to collect, use, and share data than opt-ins.

6. At the hearing, several witnesses also indicated that the Federal Trade Commission, and perhaps state attorneys general, should have primary enforcement authority for data privacy violations. In your view, what additional authority and/or resources would the FTC need to perform this function effectively?

CDT's proposal calls for an additional 100 personnel in the FTC Division of Privacy and Identity Protection.