Statement of **Justin Brookman**
Director, Privacy and Technology Policy
Consumer Reports

Before the Senate Subcommittee on Manufacturing, Trade, and Consumer Protection on

Small Business Perspectives on a Federal Data Privacy Framework

March 26, 2019

On behalf of Consumer Reports, I want to sincerely thank you for the opportunity to testify here today. We appreciate the leadership of Chairman Moran and Ranking Member Blumenthal not only for holding this important hearing, but also for working in a constructive, bipartisan fashion to develop smart and effective comprehensive privacy legislation for American consumers.

Consumer Reports is an independent, nonprofit organization that works side by side with consumers to create a fairer, safer, and healthier world. Consumer Reports has more than 6 million members and has been protecting consumers since 1936. We evaluate approximately 2,800 products and services each year, including testing for privacy and information security.

Comprehensive Privacy Legislation is Long Overdue in the United States

As an initial matter, it is important to keep in mind the fundamental reason we are debating this issue: the United States lacks any sort of comprehensive framework to protect personal privacy. The Federal Trade Commission has brought a number of important privacy and security cases over the past twenty years under its general purpose consumer protection authority, but its legal authority and resources are extremely limited. The considerable majority of its privacy cases have been under its *deception* authority, meaning the company had to affirmatively mislead consumers about their privacy practices. As a result, privacy policies tend to be extremely expansive and vague, providing very little in the way of meaningful information. Current law imposes few other checks on the collection and dissemintation of our personal information.

As a result of this lawless environment, consumers understandably feel they have lost all control or agency over their data.[1] Facebook and Google track what users do on the majority of sites around the web and across our different devices,[2] in other mobile apps,[3] and increasingly in the physical world.[4] The Weather Channel app collects personal geolocation to show you the weather where you are, and then sells that information to data brokers and hedge funds.[5] And cell carriers have been caught giving location information to various faceless middlemen, creating a virtual black market for in sensitive personal data.[6] And companies' technological ability to surveil every aspect of our lives will only increase. Policy is the only way to provide consumers with the reasonable zone of privacy they deserve.

In response to this environment, lawmakers are finally acting. Last year, California passed the California Consumer Privacy Act (the "CCPA")[7] — the first comprehensive privacy law in the United States. While key improvements are needed, the law has four basic requirements: better transparency, a right to access your information, a right to delete unneeded information, and a right to opt out of the sale of personal data. Other states — including New York,[8] Massachusetts,[9] Nevada,[10] and Washington[11] — are considering their own legislative solutions. Although Congress has passed narrowly targeted bills over the years, it has struggled to advance broader privacy legislation going back to Senator Fritz Hollings' Online Privacy

---

[1] Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, Pew Research Ctr. (Mar. 27, 2018), https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/ (noting 91% "agree" or "strongly agree" that they have lost control over how their personal information is collected or used).

[2] Justin Brookman *et al.*, *Cross-Device Tracking: Measurement and Disclosures*, Privacy Enhancing Technologies Symposium (2017), https://petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf.

[3] Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook.*, Wall St. J., (Feb. 22, 2019), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

[4] Mark Bergen & Jennifer Surane, *Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales*, Bloomberg (Aug. 30, 2018), https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales.

[5] Jennifer Valentino-DeVries *et al.*, *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.

[6] Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Motherboard (Jan. 8, 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

[7] California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798.198(a) (2018), http://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180SB1121.

[8] S. 224 (2019).

[9] S. 341 (2019).

[10] S.B. 220 (2019).

[11] S.B. 5376 (2019).

Protection Act at the beginning of this century.[12] Today, however, it seems that there is relatively universal acknowledgement that *some* new legislation is needed to safeguard personal privacy, and Consumer Reports commends the Senators for their close attention to this issue.

Privacy Legislation is About Reining in Big Tech Companies and Data Brokers — Not Small Businesses

In considering how to craft privacy legislation and its application to small businesses, it is worth keeping in mind that the primary motivation behind privacy law is to combat the excesses of big internet companies and a small number of niche companies whose primary business is trafficking in personal data.[13] The core principles and values motivating new privacy law — limiting data collection and sharing to what it reasonably necessary to deliver goods and services to consumers — shouldn't affect the core operations of the vast majority of small businesses. Notably, the examples given above about privacy violations do not involve small businesses. The ordinary collection and use of first-party data is generally permitted by most legislative frameworks; small businesses that use this information for marketing already have to comply with the reasonable requirements imposed by laws such as CAN-SPAM[14] and the TCPA.[15]

Arguably the most important element of privacy legislation is a prohibition on selling information about your customers to third-party data brokers (and for laws such as CCPA, this prohibition only applies when a consumer affirmatively opts out). However, it should be hoped that rules limiting — or at least giving consumers rights over — this behavior would not be controversial, as such sales are inconsistent with reasonable consumer expectations and constitute a violation of trust between these businesses and their customers. Yes, some small businesses — such as Cambridge Analytica and other companies who business model is predicated on accessing and selling third-party data — will be substantially affected by new privacy law: as they should be. But for most companies, privacy law should not affect their primary business model.

Privacy Law Isn't a Secret Plot to Help Google and Facebook

One curious talking point that has been aggressively pushed in DC in recent months is that privacy law actually helps companies like Facebook and Google who have more resources to develop privacy compliance regimes. The fact that this line is being pushed by groups that

---

[12] *Senate Eyes Net Privacy*, CNN (May 23, 2000), https://money.cnn.com/2000/05/23/technology/ftc_privacy/.
[13] Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley — and Won*, N.Y. Times (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html?login=email&auth=login-email.
[14] 15 U.S.C. § 7701.
[15] 47 U.S.C. § 227.

are funded by Google and Facebook[16] — and sometimes even those companies themselves[17] — calls into question how good faith this criticism is. In any event, given the consistency with which the attack is repeated, it is worth analyzing the validity of the argument.

First, the notion that privacy protections will entrench Google and Facebook is belied by the fact that Google and Facebook have consistently lobbied aggressively against nearly all proposed privacy legislation in both the United States and Europe.[18] Critics levied similar arguments that adoption of a Do Not Track system to make opting out of online data collection easier would favor those companies.[19] Again, however, both fought hard to stop industry adherence to that standard. And as a result, Google and Facebook (and the vast majority of the ad tech industry) ignore users' Do Not Track instructions on the web to this day.[20]

Certainly, if a company's business model is predicated *entirely* on bad privacy practices, then privacy legislation will especially impact them, and will probably disadvantage them more compared to companies like Google and Facebook — but that of course is their own fault. Both

---

[16] *See*, *e.g.*, Letter from TechFreedom to the Honorable Charles "Chuck" Grassley *et al.* re April 10 Senate Hearing "Facebook, Social Media Privacy and the Use and Abuse of Data," & April 11 House Hearing "Facebook: Transparency and Use of Consumer Data," (Apr. 10, 2018), http://docs.techfreedom.org/TechFreedom_Congressional_Letter-Facebook_hearing_4-10-18.pdf (noting "Facebook has been one of many supporters of TechFreedom's work"); Testimony of Roslyn Layton before the House Subcommittee on Consumer Protection and Commerce, How the US Can Leapfrog the EU — The Role of Technology and Education in Online Privacy, (Feb. 26, 2019), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Roslyn%20Layton%20Testimony%20Feb%2026%202019.pdf; Transparency, Google, https://www.google.com/publicpolicy/transparency.html (disclosing funding for TechFreedom and the American Enterprise Institute).

[17] Sheera Frenkel *et al.*, *Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis*, N.Y. Times (Nov. 14, 2018), https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html ("While Facebook had publicly declared itself ready for new federal regulations, Ms. [Sheryl] Sandberg privately contended that the social network was already adopting the best reforms and policies available. Heavy-handed regulation, she warned, would only disadvantage smaller competitors."); Sam Schechner & Nick Kostov, *Google and Facebook Likely to Benefit From Europe's Privacy Crackdown*, Wall St. J. (Apr. 23, 2018), https://www.wsj.com/articles/how-europes-new-privacy-rules-favor-google-and-facebook-1524536324, ("CEO Mark Zuckerberg recently told the U.S. Congress: 'A lot of times regulation by definition puts in place rules that a company that is larger, that has resources like ours, can easily comply with but that might be more difficult for a smaller startup.'").

[18] Carole Cadwalladr and Duncan Campbell, *Revealed: Facebook's Global Lobbying Against Data Privacy Laws*, The Guardian (Mar. 2, 2019), https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment; Taryn Luna, *Facebook, Google Spending Big Bucks to Fight Calfornia Data Privacy Measure*, Sac. Bee (Mar 23, 2018), https://www.sacbee.com/news/politics-government/capitol-alert/article206394929.html.

[19] Max Ochoa, *Why We Oppose Do Not Track and How to Fix It*, AdAge (Jul 25, 2014), https://adage.com/article/guest-columnists/oppose-track-fix/294319/.

[20] Kashmir Hill, *'Do Not Track,' the Privacy Tool Used by Millions of People, Doesn't Do Anything*, Gizmodo (Oct. 15, 2018), https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324.

Google and Facebook have problematic practices that need to be addressed by privacy rules, but both also have core products that can be monetized effectively without collecting extraneous information and compromising user privacy. However, because those companies' business models are also heavily reliant on the use of personal information, privacy law does impact them directly — and considerably more than most companies. The Federal Trade Commission has already brought actions against both companies for privacy violations, though due to weaknesses in the law and the limitations in its own authority, its actions have not sufficiently deterred their abuses.

Finally, it is premature to judge the effect of Europe's Generan Data Protection Regulation ("GDPR") — and certainly CCPA which has yet to go into effect — on big internet companies. As privacy advocates have extensively documented,[21] both companies are currently in substantial violation of GDPR's provisions; it remains to be seen whether European Data Protection Authorities will enforce GDPR after a spotty enforcement record under previous privacy regimes. However, earlier this year, the French DPA levied a €50 million fine against Google for failure to comply with GDPR[22] — and just yesterday, the Vienna Higher regional court issued a decision allowing a civil suit under GDPR to proceed against Facebook.[23] So it may well be the case that GDPR will finally start to curb the worst abuses of giant internet companies — at least in Europe.

<u>But, Privacy Law *Can* Be Written Badly to Illegitimately Help Big Companies</u>

Certainly, privacy law can be written in ways that do unfairly advantage large incumbent companies. For example, several big companies are aggressively pushing bills that predicate various privacy rights and obligations on subjective and labor-intensive *risk assessments* or *interest-balancing* that weaken consumer protections and disadvantage smaller companies without the resources to pay lawyers to conduct and document such analyses. Microsoft is pushing such a bill in Washington State (consumer advocates are universally opposed),[24] and Intel has promoted model legislation that protects consumers only when companies unilaterally determine that data processing poses a "significant" and "disproportionate" privacy risk.[25]

---

[21] Norwegian Consumer Council, *Deceived by Design*, (Jun. 27, 2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf; NOYB, *GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook*, (May 25, 2018), https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf.
[22] Jon Porter, *Google Fined €50 Million for GDPR Violation in France*, TheVerge, (Jan. 21, 2019), https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil.
[23] Press Release, *Defeat for Facebook: Vienna Court admits Model GDPR Lawsuit*, NOYB, (Mar. 25, 2019), http://schre.ms/wp-content/uploads/2019/03/PA_OLG_en.pdf.
[24] Letter of Consumer Reports *et al*. to Washington Senate Ways and Means Committee re: SB 5376 (Protecting Consumer Data) — OPPOSE, (Feb. 21, 2019), https://advocacy.consumerreports.org/wp-content/uploads/2019/02/SB-5376-Privacy-Coalition-Letter-Oppose.pdf.
[25] Legislation, Intel (last updated Jan. 28, 2019), https://usprivacybill.intel.com/legislation/.

These types of bills fail to provide needed clarity to both business and consumers, and give far too much power and discretion to companies who can hire the best lawyers to internally justify the privacy protections to decide to offer. This concept of predicating privacy protections on risk assessments is not reflected in existing privacy statutes today — for example, the Wiretap Act[26] or Video Privacy Protection Act[27] don't ask companies to conduct risk impact assessments before privacy rights apply. Laws that pair high levels of process with weak substantive provisions are the worst of both worlds for consumers, driving up prices, and advantaging bigger, established companies over potential startup competitors.[28]

Instead, privacy laws should be written simply, with clear, easy-to-understand and -apply *per se* obligations: Collect only the data you reasonably need. Don't sell data about your customers. Get rid of outdated data. Use reasonable security to safeguard data. On the other hand, privacy law should also explicitly carve out some limited first-party secondary uses of personal information — such as for internal analytics and marketing — so that companies know what is authorized by the law, and so they don't need to subject their customers to unwanted and unnecessary user prompts for consent to engage in unobjectionable practices.

Further, there is legitimate concern that large companies' outsize lobbying power and access to policymakers will lead to bad policy outcomes. During the last bout of significant interest in privacy legislation at the beginning of this decade, big internet companies were able to insert loopholes that weakened protections and safeguarded their own interests. Facebook, for example, infamously got a "Facebook exception" added to a bill proposed by Senators Kerry and McCain bill that would have shielded their most controversial data collection practices from the scope of the bill's protections.[29] And Google notoriously had a very cozy relationship with the Obama administration and as a result had an inappropriately large role in the development of their ill-fated privacy bill.[30] However, justified concern over big companies' lobbying influence does not obviate or outweigh the very real need for privacy legislation; it does, however, suggest a need for wariness and skepticism, as well as transparency and public deliberation on the part of policymakers.

---

[26] 18 U.S. Code § 2511.
[27] 18 U.S.C. § 2710.
[28] Risk assessments may be appropriate for some small subset of processing activities like the use of artificial intelligence that could have substantial and discriminatory effects on consumers (as has been proposed by Senator Wyden in his proposed privacy legislation) but few small businesses should be affected by such a requirement. *See* Press Release, *Wyden Releases Discussion Draft of Legislation to Provide Real Protections for Americans' Privacy*, (Nov. 1, 2018), https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy.
[29] Justin Brookman, *Breaking Down the Kerry-McCain Privacy Bill*, Ctr. for Dem. & Tech. (Apr. 28, 2011), https://cdt.org/blog/breaking-down-the-kerrymccain-privacy-bill/.
[30] Natasha Singer, *Why a Push for Online Privacy Is Bogged Down in Washington*, N.Y. Times (Feb. 28, 2016), https://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html.

Specific Elements of Privacy Legislation that Would Appropriately Help Small Business

In developing privacy legislation, there are a number of elements that could be included to accommodate the relative lack of resources and sophistication of small businesses. Some of these elements are outlined below:

Thresholds

First, a law could waive compliance with some subset of consumer protections for companies under a certain size. The CCPA, for example, does not apply to businesses with less than $25 million in annual revenues, who do not have data on more than 50,000 individuals, and whose primary business is not the sale of personal information.[31] Of course, size and revenue alone should not necessarily be dispositive — some relatively small business can have access to a tremendous amount of personal information. For example, at the time of its acquisition by Facebook, Instagram had only thirteen employees and negligible revenues; nevertheless, it hosted the personal information of tens of millions of users.[32] Access and deletion obligations may be good candidates for exceptions for small businesses with limited personal information; also, heightened transparency obligations might only apply to larger businesses with access to greater stores of data.[33] On the other hand, some obligations — such as a prohibition on sale of customer data and a duty to use reasonable data security — should attach regardless of the size and scope of personal information possessed by a company. Nevertheless, an assessment of what is "reasonable" for any individual company may appropriately consider a company's size and available resources (as well as other factors such as the sensitivity and scope of data in its possession).

Exempting Pseudonymous Online Data from Access and Deletion Requirements

Other provisions in a thoughtful privacy law could make compliance easier for small companies. For example, while a privacy law should apply broadly to a wide range of information — including online data associated only with a cookie or IP address — exempting certain data from access requests would ease the burden of compliance, prevent illegitimate access to personal information in shared environments, and incentivize companies to maintain in less identifiable forms. While most of a law's protections would apply to device-level or household-level data (such as transparency and a prohibition on sale), those types of data could

---

[31] CCPA, § 1798.140(c).

[32] Victor Luckerson, *Here's Proof That Instagram Was One of the Smartest Acquisitions Ever*, Time (Apr. 19, 2016), http://time.com/4299297/instagram-facebook-revenue/

[33] Comments of Consumer Reports to the National Telecommunications and Information Administration re Re: Docket No. 180821780-8780-01, Request for Comment on the Administration's Approach to Consumer Privacy, (Nov. 9, 2018), pp. 6-7 https://advocacy.consumerreports.org/wp-content/uploads/2018/11/CU-NTIA-Docket-No.-180821780-8780-01.pdf (comments on appropriate role of transparency in privacy legislation).

be exempted from deletion and access requirements. This is justified on policy as well as burden grounds since such data cannot reliably be authenticated, so companies could not confidently know data they possess actually pertains to a requestor. Currently, this is an issue being considered in California with regard to the CCPA, and Consumer Reports and other advocates have urged the Attorney General to promulgate rules stating that data linked only to pseudonymous identifiers (like cookies, device identifiers, households, or IP addresses) should be broadly exempt from access requests.[34]

Similarly, a privacy law could explicitly state that companies need not collect or retain additional data in order to comply with a privacy law. This too is currently a contested issue with the CCPA, as several trade associations have asserted this is a concern with the law.[35] This was certainly not the intent of the CCPA drafters and is based on a questionable reading of the statute; still, clarifying that companies don't have an obligation to engage in more invasive tracking in order to comply with privacy legislation should be noncontroversial.

Put Compliance Obligations on Tracking Companies — Not Websites

Privacy law can also be constructed to transfer compliance obligations from small publishers to the large data broker and tracking companies who are the primary target and concern of the law. For example, in response to petitions from privacy advocates,[36] the Federal Trade Commission in 2010 proposed a "Do Not Track" system to empower users to stop — or at least substantially curtail — online behavioral tracking.[37] Major browser companies created a setting that allowed users to broadcast a Do Not Track signal as they surfed the web. Importantly, this system did not impose any obligations on websites themselves — just on the third-party tracking companies that monitored user behavior across different sites.[38] In 2012, the

---

[34] Comments of Consumer Reports re Rules Implementing the California Consumer Privacy Act at 4-5 (Mar. 8, 2019), https://advocacy.consumerreports.org/wp-content/uploads/2019/03/CR-CCPA-Comments-to-CA-AG.pdf. It might also be appropriate to exempt data that could be used for identity theft from access requirements, as the utility to consumers is marginal, and the potential abuses considerable.

[35] Wendy Davis, *ANA Presses California To Refine Privacy Law*, MediaPost (Feb. 15, 2019), https://www.mediapost.com/publications/article/331560/ana-presses-california-to-refine-privacy-law.html (arguing "'[t]he CCPA could have the unintended effect of forcing business to associate non-identifiable, pseudonymized device data with a specific person seeking to exercise their CCPA rights'").

[36] *Online Behavioral Advertising Moving the Discussion Forward to Possible Self-Regulatory Principles*, Fed. Trade Comm'n (Dec. 20, 2007), https://www.ftc.gov/public-statements/2007/12/online-behavioral-advertising-moving-discussion-forward-possible-self.

[37] Ira Teinowitz, *Chairman: FTC Leans Toward "Do Not Track" Registry*, Ad Age (Jul. 27, 2010), https://adage.com/article/news/chairman-ftc-leans-track-registry/145131/.

[38] The Do Not Track system was proposed to address the myriad deficiencies in extant industry opt-out programs, including lack of universal applicability, failure to address data collection and retention, and technological limitations. For more on the history of Do Not Track and the inadequacy of industry self-regulatory efforts, *see* Testimony of Justin Brookman Before the House Subcommittee on Digital Commerce and Consumer Protection on Understanding the Digital Advertising Ecosystem, (Jun. 14, 2018),

major ad tech trade associations publicly committed to honoring Do Not Track settings;[39] however, within a handful of years, they had completely reneged on their promises.[40] Today, users' Do Not Track instructions are nearly universally ignored. This failure of industry to respond in good faith to users' privacy settings highlights the need for this body to advance privacy legislation. In order to achieve what Do Not Track ultimately failed to do, a privacy law could include a mandate that third-party vendors adhere to users' stated privacy preferences, while absolving website publishers from any obligations other than to pass those signals along to tracking services.

Provide for Data Portability and Interoperability to Allow Small Providers to Compete with Larger, Incumbent Players

Finally, strengthening consumer agency with regard to their own data can also promote competition and market choice. Data portability and interoperability requirements can accomplish both important policy goals by giving consumers control over their data while helping small businesses compete with big companies. While data portability allows consumers to take their data to innovative and privacy-protective new services, it can only be accomplished when the digital ecosystem is interoperable. In its report on "Unlocking Digital Competition," the United Kingdom's Digital Competition Expert Panel found that, "the development of common standards for sharing data has huge potential to improve consumer choice and boost competition."[41] Indeed, requiring interoperability protocols can facilitate competition in the face of the strong network effects that make consumers feel locked into dominant incumbents.

Conclusion

For good actors, privacy law should be straightforward to comply with: ordinary, first-party data collection and processing for fulfilling customer orders — as well as expected operational uses like analytics, fraud prevention, and even marketing — should be generally allowed, without forcing consumers through unnecessary consent dialogs and permission requests. Companies will still have some obligations — notably, not to sell customer data and to use reasonable data security — but at least the latter is already required by a growing number of state security laws as well as existing prohibitions on unfair and deceptive practices. Bigger

---

https://docs.house.gov/meetings/IF/IF17/20180614/108413/HHRG-115-IF17-Wstate-BrookmanJ-20180614.pdf.

[39] Rainey Reitman, White House, Google, and Other Advertising Companies Commit to Supporting Do Not Track, Elec. Frontier Found., (Feb.23, 2012), https://www.eff.org/deeplinks/2012/02/white-house-google-and-other-advertising-companies-commit-supporting-do-not-track.

[40] Kashmir Hill, *'Do Not Track,' the Privacy Tool Used by Millions of People, Doesn't Do Anything*, Gizmodo, (Oct. 15, 2018), https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324.

[41] Jason Furman *et al.*, *Unlocking Digital Competition — Report of the Digital Competition Expert Panel*, (Mar. 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.

companies should be expected to respond to access and deletion requirements, but the bulk of these requests will be directed at the internet giants who have the power and scale to build up rich, detailed profiles about consumers. Privacy legislation is primarily designed to check the power of these dominant companies — as well as data brokers who specialize in trafficking personal data. Ultimately, a well-written privacy law should tilt the balance of power in favor of smaller companies whose business models aren't predicated upon tracking every aspect of consumers' lives.