Before the
Federal Trade Commission
Washington, DC 20580

In the Matter of	)	
	)	
Competition and Consumer Protection	)	Docket No. FTC-2018-0098
in the 21st Century Hearings: The FTC's	)	
Approach to Consumer Privacy	)	

COMMENTS OF NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE

Eric Null
Becky Chao
Sharon Bradford Franklin
New America's Open Technology Institute
740 15th Street NW
Suite 900
Washington, DC 20005

May 31, 2019

TABLE OF CONTENTS

I. Introduction

New America's Open Technology Institute (OTI) submits these comments in response to the Federal Trade Commission's (FTC) request for comments on FTC Hearing #12: the FTC's Approach to Consumer Privacy.

The current privacy approach, based primarily on notice and consent, falls short in preventing harmful data practices and protecting users' privacy. Without robust baseline requirements, the regime grants companies wide discretion in setting their own policies, leaving users on their own to determine their willingness to consent. Critically, notice and consent places an untenable burden on consumers. Surveys have long supported the idea that users value privacy, but requiring them to interpret every data policy from each company they interact with and make informed decisions based on their individual privacy preferences is exhaustive and burdensome. Should the FTC continue to push for a notice and consent regime, at the very least it should require companies to provide straightforward notices directly to users while giving far more detailed notice to regulators and watchdog organizations. But without additional changes, like the addition of user controls and imposing data limits on companies, any notice and consent regime is insufficient.

A consumer privacy regime must incorporate company requirements, user rights, and strong enforcement. Companies should be required to minimize the total amount of data they collect, use, and store, and justify why they collect that data and how they use it. In addition, companies should be restricted from using data for secondary and discriminatory uses. Users should have the right controls enabling them to access, correct, delete, and port data. Further, strong enforcement, including from the FTC, is necessary to hold companies accountable to a privacy regime.

The FTC should remain open to imposing additional privacy requirements on broadband providers. Broadband providers are sufficiently different from other online companies to merit specifically-tailored privacy rules. They have nearly comprehensive access to all traffic that flows over their networks, and therefore, present enormous risks associated with the potential misuse of this data.

II. The federal privacy regime must move beyond notice and consent

For twenty years, the U.S.'s approach to protecting privacy has relied primarily on notice and consent. Not only does this approach fail to prevent harmful data practices, it also places an unsustainable and unreasonable burden on users. Users want more control over the data they provide companies, but often find it difficult to navigate endless legalistic privacy policies they confront daily and make informed decisions based on their individual privacy preferences. Even if notice and choice remains a key aspect of the federal privacy regime, it should require two-tiered notice such that there is an extra level of notice provided to regulators and other watchdogs to hold companies accountable.

The federal privacy regime of notice and consent has failed to address users' actual privacy concerns and prevent harmful data practices. Requiring notice and consent only requires companies to be non-deceptive in their privacy policies. This approach grants companies wide discretion in setting their own policies, with few baseline requirements, and users in theory determine their willingness to agree. The regime does not allow users to protect themselves against particular practices they may not agree with or desire, and it is not a realistic option for consumers to opt out of using many products and services. While competitive markets may incentivize some companies to compete on privacy, several of the most popular services, like Facebook's social network, lack robust competitors.[1]

Survey data supports the idea that notice and consent places an untenable burden on individual users. While users care about their privacy, requiring them to interpret every notice and data policy from each company they interact with and make informed decisions that align with their personal privacy interests is both tiring and burdensome. A Pew Research Center survey from early 2015 found that a sizable number of U.S. adults said they were confused by the information companies chose to share in privacy policies, discouraged by the amount of effort needed to understand the implications of sharing their data, and impatient because they felt rushed to make an immediate decision despite wanting to take the time to learn more.[2] This has

[1] See, e.g., Dina Srinivasan, Why Privacy is an Antitrust Issue, The New York Times (May 28, 2019), https://www.nytimes.com/2019/05/28/opinion/privacy-antitrust-facebook.html.
[2] Americans are conflicted about sharing personal information with companies, Pew Research Center (Dec. 30, 2015),

led to users feeling resigned to giving up their privacy in exchange for the use of online services.[3]

Ultimately, users want more control over their data.[4] According to a PwC survey conducted in 2017, 92% of users in the U.S. believe they should be able to control the information available about them on the internet, but only 10% feel they have complete control over their personal information.[5] Further, survey after survey has found that users have growing anxiety over data privacy and security. A survey conducted in October 2018 by Survey Monkey for Anagog found that users are wary of handing over control of their data: 83% of respondents were concerned the mobile apps they download automatically collect their personal data, and over 80% were concerned that companies collect their mobile data and share it with third parties.[6] Security is also top of mind for the majority of users, with 85% of survey respondents stating that they are wary about sharing photos, posts, and updates about their current location due to potential security risks.[7] A survey by the Harris Poll on behalf of IBM conducted in March 2018 found that 85 percent of users think companies should be doing more to actively protect their data, and that 73 percent believe businesses are focused on profits over users' security needs.[8]

GDPR is another example of why notice and consent insufficiently protects users. The regulation has been widely criticized for its vague consent notice requirements that have been widely interpreted across different companies.[9] Companies have implemented default pre-ticked

---

https://www.pewresearch.org/fact-tank/2015/12/30/americans-conflicted-about-sharing-personal-information-with-companies/.

[3] Joe Turow, et al., The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation (June 26, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820060.

[4] Reply Comments of New America's Open Technology Institute, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Dkt. 16-106, at 21-27, https://ecfsapi.fcc.gov/file/10707717014775/2016-07-06%20-%20OTI%20Broadband%20Privacy%20Reply%20Comments%20FINAL.pdf.

[5] Consumer Intelligence Series: Protect.me, PwC, https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html.

[6] Consumer Privacy Survey Shows 70% Want Personal Data to Stay on Mobile Phones, Business Wire (Nov. 13, 2018), https://www.businesswire.com/news/home/20181113005171/en/Consumer-Privacy-Survey-Shows-70-Personal-Data.

[7] *Id*.

[8] IBM Cybersecurity and Privacy Research, The Harris Poll (Apr. 13, 2018), https://newsroom.ibm.com/Cybersecurity-and-Privacy-Research.

[9] Jessica Davies, 'Everyone is breaking the law right now': GDPR compliance efforts are falling short, Digiday (June 28, 2018), https://digiday.com/media/everyone-breaking-law-right-now-gdpr-compliance-efforts-falling-short/.

opt-in consent-request messages, which feature prominently the option to accept, but bury the option not to.

Should the FTC continue to push for a notice and consent regime, at the very least, the FTC should require companies to provide straightforward notices directly to users while giving far more detailed notice to regulators and watchdog organizations.[10] In this two-tiered notice regime, users would receive a high-level description of what the company *actually does* (as opposed to what it "may" do) with the data, while a second privacy notice would provide a detailed description of what the company actually does with data for regulators and watchdog organizations to ensure that the companies meet their more detailed promises. Both types of notices are important because users are more likely to read high-level privacy policies than lengthy and detailed notices, while companies at the same time need to be held accountable for their actual data practices.

The U.S. privacy regime must move beyond notice and consent. But if the FTC continues to center notice and consent, the above minimum changes can provide some improvement over the current regime. But without larger changes, like the addition of user controls and imposing data limits on companies, any notice and consent regime is insufficient.

III. Company requirements, user rights, and strong enforcement should be central to any approach to consumer privacy

A federal privacy regime should place emphasis on company requirements, user rights, and strong enforcement. Companies should have real, substantive requirements for data minimization and use restrictions. Users should have rights to access, correct, delete, or port data depending on the type of data. Companies must also be held accountable for privacy violations.

A. Companies should have substantive requirements for data minimization and use restrictions

A federal privacy regime should include data minimization requirements and use restrictions. Companies should minimize the data they collect and retain, and also justify why they collect that data and how they use it. Further, companies should be restricted from using

[10] See, e.g., Free Press/Lawyer's Committee privacy bill Sec 7(b)-(c), https://www.freepress.net/sites/default/files/2019-03/online_civil_rights_and_privacy_act_of_2019.pdf.

data unfairly, such as for secondary purposes that users do not consent to, and for discriminatory purposes.

1. Data minimization benefits users and companies

Data minimization—the practice of reducing the total amount of data collected, used, and stored—*must* play a prominent role in a privacy regime. Companies should not only minimize the data they collect and retain, but also justify why they collect that data and how they use it. Thus, data should be collected only for business purposes, and data should be retained for a limited amount of time by default.

Data minimization has several benefits. First, data minimization reduces the risks associated with data collection and storage, such as data breaches and other unauthorized access. [11] As the IAPP has stated, "we are all suffering from data overload" and "more data means more problems; the hackers and data thieves couldn't be happier."[12] Data breaches can be ruinous for companies, and the more data companies have about their users, the higher the likelihood that they will be a target and that a breach would have catastrophic consequences.[13]

Second, collecting too much data, including data extraneous to a business need, increases privacy risks, such as inappropriate secondary uses and discriminatory uses that are detailed in the following section. For instance, Google's Street View mapping cars collected data over unprotected Wi-Fi networks for years, amassing sensitive data including telephone numbers, passwords, e-mail, text messages, medical records, and more—this data was unnecessary for mapping, and could have easily been repurposed for inappropriate secondary uses.[14] Data minimization offers another layer of protection for users by limiting companies in their collection and storage of personal data that might be used to discriminate against, manipulate, or profile individuals.

---

[11] See FTC Staff Report: Internet of Things: Privacy & Security in a Connected World, Federal Trade Commission (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (at IV)

[12] Reducing Risk Through Data Minimization, International Association of Privacy Professionals, https://iapp.org/resources/article/reducing-risk-through-data-minimization

[13] Bernard Marr, Why Data Minimization is an Important Concept in the Age of Big Data, Forbes (Mar. 16, 2016), https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-ageof-big-data/#7bd907211da4.

[14] David Kravets, An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle, Wired (May 2, 2012), https://www.wired.com/2012/05/google-wifi-fcc-investigation/.

Third, it reduces the amount of information a company has to convey to its users. Users can only read, understand, and internalize a limited amount of information about data practices at a time. Already, our privacy regime incorrectly assumes that users read privacy policies. A Deloitte survey found that 91% of users consent to terms of service without reading them.[15] If informing users continues to be a central pillar of our privacy regime, the amount of information they are required to absorb must be reduced.[16] In addition to implementing the two-tiered privacy regime as discussed above, reducing data collection and retention will help reduce the burden on the user of staying informed.

Finally, data minimization reduces costs for companies, as they no longer have to maintain such extensive data collection and storage systems.[17] Collecting, storing, and using data is costly.[18] And sifting through large amounts of data to find the needle in the haystack can increase costs as well: "the dangers of data hoarding are similar to those of physical hoarding: mounds of useless junk that make it very difficult to find what we need when we need it. It costs money and time...."[19] Processing less data means reducing spending on processing data.

As a result of these benefits, minimizing data collection, use, and storage will likely increase trust between users and companies, to the benefit of both.

2. Companies should be restricted from using data for secondary and discriminatory uses

Companies should be restricted from engaging in certain types of data practices that are inherently unfair. In thinking about new privacy approaches, the FTC should consider applying use restrictions with limits on secondary uses of data and limits on discriminatory uses.[20]

---

[15] Caroline Cakebread, You're not alone, no one reads terms of service agreements, Business Insider (Nov. 15, 2017), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11.
[16] Currently, if users want to stay informed about their privacy choices, it could take up to 304 hours per year of time to read those policies. Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf (at 17).
[17] *Id.*
[18] Shantha Kumari, Data Minimization in the Age of Big Data!, Sysfore Blog (Apr. 22, 2016), https://blog.sysfore.com/data-minimization-in-the-age-of-big-data.
[19] Bernard Marr, Why Data Minimization is an Important Concept in the Age of Big Data, Forbes (March 16, 2016), https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-ageof-big-data/#7bd907211da4
[20] See, e.g., CDT's Federal Baseline Privacy Legislation Discussion Draft, Center for Democracy and Technology (Dec. 13, 2018), https://cdt.org/insight/cdts-federal-baseline-privacy-legislation-discussion-draft/.

A privacy regime should preclude use of data to discriminate based on a protected class or take actions that have a disparate impact on marginalized communities. The digital economy has enabled new means of perpetuating discrimination by using people's personal data, and a privacy regime should not exacerbate those problems. For instance, numerous studies have found that Facebook's ad delivery algorithm discriminates based on race and gender. ProPublica in 2016 found that Facebook allowed advertisers to place ads for housing or job postings that excluded people based on race using the personal data the company had collected about its users. [21] Even after Facebook removed those advertising options, another study published in April 2019 found that discrimination along racial and gender lines persisted in Facebook's job listings and housing ad delivery—even when advertisers tried to reach a broad audience and did not opt to target specific demographics.[22] As for algorithms and machine learning more generally, the FTC should require more transparency to help determine when a disparate impact exists.

The same way that data can be manipulated to exclude people from certain goods and services, data can also be manipulated to price discriminate based on individuals' protected class status.[23] For example, Amazon has offered free same-day shipping to its "best" customers, using zip codes to determine availability that skewed toward white customers, forcing communities of color to pay higher shipping costs.[24] Some retailers have also used data on users' physical location to charge higher online prices and offer fewer deals for people in low-income neighborhoods,[25] which are often people of color and particularly Black people.

Secondary uses of data can also be problematic. With little to stop companies from engaging in secondary uses that users likely do not understand, some companies have collected data without clearly disclosing what data specifically is being collected and why, and have repurposed this data for secondary uses without explicit consent. For instance, Facebook

[21] Julia Angwin & Terry Parris Jr., Facebook Lets Advertisers Exclude Users by Race, ProPublica (Oct. 28, 2016), https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race.
[22] Muhammid Ali, et al. (2019), Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes, https://arxiv.org/abs/1904.02095.
[23] See Cassandra Jones Harvard, On the Take: The Black Box of Credit Scoring and Mortgage Discrimination, Pub. Int. L.J. 20 (2011): 271.
[24] David Ingold and Spencer Soper, Amazon Doesn't Consider the Race of Its Customers. Should it?, Bloomberg (April 21, 2016), https://www.bloomberg.com/graphics/2016-amazon-same-day/.
[25] Jennifer Valentino-DeVries, Jeremy Singer-Vine, & Ashkan Soltani, Websites Vary Prices, Deals Based on Users' Information, The Wall Street Journal (Dec. 24, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534?ns=prod/accounts-wsj.

repurposed users' phone numbers originally collected as part of a two-factor authentication security protocol against unauthorized logins to deliver targeted advertising to users—a secondary use that users did not consent to.[26] Wearable technology companies also collect health data that may be used for secondary applications, like emotional marketing.[27] Companies like mPath have already leveraged data collected by wearable stress sensors, analytics, and other technologies to determine consumer responses to marketing strategies.[28]

B. Users should have the right to access, correct, delete, and port data

Users should have the broadest data rights possible in a privacy regime. Users should have easy-to-use, easy-to-find controls, and the ability to access, correct, and delete data that a company has collected from or about them. User controls must also include broad access to data portability. Unlike a notice regime, these rights are tangible, giving users the ability to actually see what data any particular company has about that user, and gives that user options to take action. Or, a user may determine the company has too much data, and may discontinue using the service. Either way, providing more concrete information to the user is a good thing.

In determining which types of data can be accessed, corrected, ported, or deleted, it is useful to think about the following taxonomy of collected data: 1) data that a user directly provides a company (including data uploaded to a service by the user), 2) data provided to the company by a user and created collaboratively with other users, 3) data that concerns or pertains to a user collected by the company through use of service (passively collected data), 4) data that concerns or pertains to a user and collected by the company via a third party such as a data broker or advertiser, and 5) data that a company infers about a user. The extent of user rights may vary based on type of data.

First, users should have a right to access essentially all data a company collects on them by default, with only rare exceptions for data that would be actively harmful to the company to

[26] Natasha Lomas, Yes Facebook is using your 2FA phone number to target you with ads, TechCrunch (Sept. 27, 2018), https://techcrunch.com/2018/09/27/yes-facebook-is-using-your-2fa-phone-number-to-target-you-with-ads/.
[27] Gicel Tomimbang, Wearables: Where do they fall within the regulatory landscape?, IAPP (Jan. 22, 2018), https://iapp.org/news/a/wearables-where-do-they-fall-within-the-regulatory-landscape/.
[28] Rob Matheson, Wearable device reveals consumer emotions, MIT News (July 12, 2017), http://news.mit.edu/2017/wearable-device-reveals-consumer-emotions-0712.

disclose. With regard to the video game hypothetical discussed at the FTC hearing,[29] the user should have access to all the listed data, including the inference that the user might be cheating. Users may find it useful to know that the company collects and retains such information. Knowing whether the company thinks the user is likely to make in-app purchases may help the user curb that behavior or help the user better understand their financial decisions. Knowing the company thinks the user cheats may lead the user to try to correct the record, or the user may quit the game entirely if the inference is unfair. In a very small number of instances, allowing access to this type of information may allow an actual cheater to better hide their cheating, but that is an insufficient reason to hide this type of information from users broadly. Users should know about such inferences so the user can decide whether to continue playing the game.

Second, users should have a right to correct data, especially when that data is being inferred from other (raw) data and a company is making decisions about users based on that data. [30] In the video game hypothetical above, a user may have an interest in correcting the record on something like whether the user is cheating, especially if that designation has led to more in-game monitoring, or may lead to a suspension of the user's account.

Third, users should have a right to delete data. This right may be the most limited, but data should in general be deletable. A user should have the ability to remove data from a service that they no long want associated with that service provider. And when a user deletes their account, that action should delete (rather than de-identify) the data associated with that account as much as that is feasible.

Last, users should have the right to port data. Data portability is critical to ensuring that users have control over their data. Over the past several years, private companies have trended toward locking down their data rather than opening it up. This trend further entrenches tech

---

[29] Competition and Consumer Protection in the 21st Century: The FTC's Approach to Consumer Privacy, Federal Trade Commission (April 10, 2019), https://www.ftc.gov/system/files/documents/public_events/1418273/ftc_hearings_session_12_transcript_day_2_4-10-19.pdf. ("Company X is a video game company. It allows gamers to join group games, make in-app purchases. It collects some information directly from consumers, email, user name, country, profile picture. Users can build profile pages, allow other users to comment, tag photos, private message. And as consumers interact with the games and other players, the company collects metrics about purchase transactions, history, games played, screen time ranking, maybe even IOT device use and scores. The company generates inferences about the consumers, such as skill level, low/high, in-app purchaser, risk taker, and the likelihood that the consumer cheats.")

[30] Technical data, such as clicks or times of access, does not need to be correctable.

companies in the market by making it harder for consumers to switch services or leverage their own data elsewhere. But to improve the competitive landscape, the FTC should work toward creating opportunities for data portability.[31]

C. Companies must be held accountable for privacy violations

Companies should be held accountable for their privacy transgressions. Without accountability, any privacy regime falls apart because there are essentially no consequences for violating the standards or rules put in place. Users need more, not less, enforcement.[32] When companies know that they can get away with violating the rules without punitive action, there is no deterrent. The FTC should be emboldened to seek civil penalties for privacy and data security violations in the first instance, and it should be provided more resources to accomplish its mission.[33] State attorneys general, who play an extremely important role in protecting user privacy,[34] must continue to be empowered to enforce their laws against transgressors.

Further, all enforcers should work coextensively and concurrently to ensure the maximum privacy protections. The FTC should coordinate with other federal agencies like the NTIA on enforcement and identify ways to strengthen privacy protections. Federal agencies should also work with state attorneys general to offer guidance and aid where possible.

IV. The FTC should remain open to imposing additional privacy requirements on broadband providers

Broadband providers are sufficiently different from other online companies to merit privacy rules tailored to them, an idea Congress itself established when it passed the 1996 Telecommunications Act, which identified network providers as a separate sector deserving of its own privacy rules.[35] The broadband provider versus online company debate played out at the

[31] See Comments of New America's Open Technology Institute, Competition and Consumer Protection in the 21st Century: The Intersection Between Privacy, Big Data, and Competition (filed Aug. 20 2018).
[32] Consumer Data Privacy: Examining the European Union's General Data Protection Regulation and the California Consumer Privacy Act, Hearing before the Senate Committee on Commerce, Science, and Technology (Oct. 10, 2018), Testimony of Laura Moy, https://perma.cc/3HDL-9ZY5 (at 10-14).
[33] Current FTC Chair Joseph Simons has discussed the limits of Section 5 of the FTC Act, particularly that it does not provide for civil penalties, in capturing all privacy and data security concerns in testimony before the House Committee on Energy and Commerce in a hearing on Oversight of the Federal Trade Commission on July 18, 2018.
[34] Danielle Keats Citron, The Privacy Policymaking of State Attorneys General, 91 Notre Dame Law Review 747 (Feb. 16, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733297.
[35] 47 U.S.C. §222.

Federal Communications Commission (FCC), while the agency and the public deliberated over broadband privacy.[36] Among the reasons they deserve their own privacy rules is that they have nearly comprehensive access to all traffic that flows over their networks including, in some cases, content. Broadband providers routinely collect data on users' geo-location, web browsing and app usage history, and more.[37] The risks of misusing this data are enormous: they can be used for aggressive product marketing and exploited by identity thieves, for example.[38] Broadband customers generally cannot refuse to provide data to their providers because it is needed to provide the service, and there are few, if any, direct competitors. Further, broadband providers are third parties to communications between a user and the content they seek online, making privacy violations by their broadband providers based on their control over the infrastructure unexpected and unreasonable.

The New School's Digital Equity Laboratory has found that consumers are left with a "take-it-or-leave-it" choice when purchasing internet services, largely because providers do not disclose sufficient information for users to make informed choices about privacy.[39] Specifically, the Digital Equity Laboratory found that eleven major broadband providers in New York—four residential providers (RCN, Verizon, Optimum/Altice, and Spectrum) and seven mobile providers (AT&T, Verizon Wireless, US Cellular, Metro PCS, T-Mobile, Boost Mobile, and Sprint Mobile)—generally employ language that is legally vague, with little specificity into their data practices for collection and use.[40] In addition, users are generally not notified about broadband providers' data collection.[41] Instead, their data is harvested and aggregated without their informed consent, and users lack the option to opt-out for particularly sensitive data.[42] Users were also not informed about broadband providers' procedures in case of a data breach, and are not offered detailed explanation into providers' security audits and practices. In its 2019

[36] Comments of New America's Open Technology Institute, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Dkt. 16-106, at 3-11, https://ecfsapi.fcc.gov/file/60002081381.pdf.
[37] Broadband Privacy: What Consumers Need to Know, Consumers Union (Sept. 20, 2017), https://consumersunion.org/research/broadband-privacy-what-consumers-need-to-know
[38] *Id.*
[39] Take it or Leave it: How NYC Residents are Forced to Sacrifice Online Privacy for Internet Service, The New School's Digital Equity Laboratory (June 2, 2018), https://www.digitalequitylab.org/take-it-or-leave-it/.
[40] *Id.*
[41] *Id*.
[42] *Id.*

Corporate Accountability Index, Ranking Digital Rights scored telecommunications company AT&T only 49% on privacy based on indicators that address how transparent companies are about what they do with user data, with whom they share it, and what they do to secure it.[43]

V. Conclusion

OTI commends the FTC for its ongoing efforts to examine its approach to consumer privacy. The current regime of notice and consent leaves consumers insufficiently protected against the harms that privacy violations pose, and it is clear that additional changes are needed. These changes include clear company requirements for data minimization and use restrictions, user rights, and strong enforcement. We look forward to working with the FTC as it further develops its approach.

[43] 2019 Ranking Digital Rights Corporate Accountability Index, Ranking Digital Rights (May 2019), https://rankingdigitalrights.org/index2019/.