November 9, 2018

David J. Redl
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
1401 Constitution Ave NW
Washington, DC 20230

Re: Request for Comments on Developing the Administration's Approach to Consumer Privacy, Docket No. 180821780-8780-01

Dear Assistant Secretary Redl:

On behalf of Asian Americans Advancing Justice-AAJC, Common Cause, the National Hispanic Media Coalition (NHMC), the National Urban League (NUL), and OCA-Asian Pacific American Advocates, we write today in response to the National Telecommunications and Information Administration's (NTIA) Request for Comment (RFC).[1] Through the RFC, NTIA has requested input on ways to protect and advance consumer privacy, while simultaneously protecting and advancing innovation. We submit these comments on behalf of the millions of Americans and communities of color that we represent: groups and individuals who continue to find themselves adversely impacted or completely left out of the benefits and advantages so many have enjoyed in the digital revolution.

We see privacy as both a human and civil right. While it is not explicitly outlined in the Constitution, it is embedded in the values that led to the birth of our nation and a right we should guard jealously.[2] In a digital society, that right extends to personal data collection and information sharing which creates an individualized digital footprint of each American.

Advances in technology and data collection techniques have increased our ability to connect and collaborate. Likewise, it has heightened exposure to data sharing abuses and related harms. In underserved and underrepresented communities, privacy violations can exacerbate the stigma and economic hurdles that these communities already face. Now that our digital footprints can be tracked, shared, and manipulated by public and private entities in ways that were once unimaginable, it is time to design a regulatory framework that codifies privacy protections.

Our comments are intended to set a baseline for comprehensive privacy rules that protect and serve stakeholders that rely on the Internet. The communities that we represent include communities of color, the low-income, and the disconnected. Strong privacy protections will help foster greater participation in all aspects of the online ecosystem, allowing those who have traditionally been at the margins of society to harness the potential and power of the Internet and enjoy the full potential of America's economic and democratic ideals.

---

[1] *Developing the Administration's Approach to Consumer Privacy*, Request For Comment, 83 Fed. Reg. 48600 (Sept. 26, 2018).
[2] *See* Michael Price, *Remember Why We Have the Fourth Amendment*, Brennan Center For Justice, Nov. 25, 2015, https://www.brennancenter.org/blog/remember-why-we-have-fourth-amendment.

Civil rights advocates are particularly concerned about an individual's right to control how personal information is collected and shared, both a prerequisite to ensuring that an individual's digital footprint remains intact. Consumers should have the right to choose what type of personal information is being collected, the right to see what information is stored, as well as the right to know when that information has been improperly shared. With these values as its core, our comments focus on elements of the RFC that are of the greatest concern to communities of color. We urge the NTIA to incorporate these comments into its recommendations to the Executive branch as they allow for the benefits of innovation and prosperity to be enjoyed by the greatest number of Americans.

TRANSPARENCY OF PRIVACY POLICIES MUST BE ENHANCED AND ACCESSIBLE TO COMMUNITIES OF COLOR

Transparency allows consumers to understand the purpose and extent of data collection. It is also a precondition to assessing the risks of disclosure in light of the safeguards in place. Without it, a consumer cannot offer educated consent or have any control over data utilization. Further, terms of service and legal privacy policies should be easily accessible. Companies should be required to provide simple, plain language privacy notifications or disclosures to summarize how they collect, store, use, and share personal data.

The current privacy policy paradigm creates a culture of uninformed consumers. Many consumers simply do not understand online privacy disclosures. Oftentimes, those policies require a college reading level to comprehend,[3] assuming that the privacy policy is even available for review. Thus, companies should be required to simplify disclosure notifications, using graphics and images whenever helpful, to help alleviate this problem.

In order to establish full privacy transparency among the public, policies and notifications must also be available in various languages. For example, Asian American and Pacific Islander communities encompass over 100 different languages and 50 ethnic groups.[4] In the aggregate, one third of Asian Americans have limited English proficiency and some ethnic subgroups have even less.[5] Just as companies allow consumers to change the language setting on their platforms, web pages containing privacy disclosures should be required to be readable by translation software.

Approximately 35 million U.S. citizens, making up 15 percent of the adult population, speak a language other than English at home.[6] At a minimum, companies should be required to make

---

[3] *See* Tom Calver and Joe Miller, *Social site terms tougher than Dickens*, BBC, July 6, 2018, https://www.bbc.com/news/business-44599968.

[4] *Snapshot: Asian American, Native Hawaiian, and Pacific Islander Health*, Asian & Pacific Islander American Health Forum (rel. Sept. 2017), at 1, https://www.apiahf.org/wp-content/uploads/2017/09/September2017_SnapshotAANHPIHealth_Factsheet_0-1.pdf.

[5] *Id.*

[6] *See* Christopher Ingraham, *Millions of U.S. citizens don't speak English to one another. That's not a problem*, Wash. Post, May 21, 2018, https://www.washingtonpost.com/news/wonk/wp/2018/05/21/millions-of-u-s-citizens-dont-speak-english-to-each-other-thats-not-a-problem/?utm_term=.133bf13cccdf.

web pages containing privacy disclosure readable by translation software. This would help ensure that the right to privacy extends beyond communities that are fluent in English, and reach a greater number of online users. Additionally, companies should be incentivized to provide additional language support, allowing users an opportunity for effective notice.

NOTICE HELPS CONSUMERS UNDERSTAND WHAT AND HOW PERSONAL DATA IS USED AND SHARED

Consumers have the right to know what information is being collected and have a reasonable understanding of how that information will be used or shared. They should also receive timely and adequate notifications when a security breach exposes personal data. Notably, previous administrations have supported a regulatory framework that require a company to obtain informed consent in order to collect, monetize, and share personal data.

For instance, in 2012, the Executive branch supported a consumer Bill of Rights that identified a baseline for consumer privacy protections.[7] The proposal was based on universally accepted Fair Information Practice Principles (FIPPs) and started with the individual control principle which identified a consumer's right to exercise control over what personal data would be collected and how that information would be used.[8] Incorporating those principles would help ensure consumers, especially those in vulnerable populations, remained the primary beneficiaries in any regulatory framework.

CONSUMERS SHOULD HAVE THE OPPORTUNITY TO CONSENT TO THE COLLECTION, USE, OR SHARING OF PERSONAL DATA

Voluntary participation in data collection requires informed consent. To that end, companies should be required to disclose information about its data collection in language that is easy to understand so that consumers are able to decide whether or not to offer consent. As the General Data Protection Regulation (GDPR) adopted by the European Union rightly states, consent should not only be given specifically and unambiguously, but consumers should be able to withdraw consent easily and without detriment.[9] Currently, in the U.S. marketplace, users are often given a choice between sharing information and protecting their privacy or losing access to a platform entirely.[10] Privacy regulations should ensure consumers have choices about how their data is used and shared without losing access to tech platforms.

---

[7] *See generally Consumer Data Privacy in a Networked World: A Framework for Protecting Intellectual Privacy and Promoting Innovation Enforcement in the Global Digital Economy*, The White House (rel. Feb. 23, 2012), https://www.hsdl.org/?view&did=700959.

[8] *Id*. at 1.

[9] *See* Sally Annereau, *Understand consent under the GDPR*, Global Data Hub, Nov. 2016, https://globaldatahub.taylorwessing.com/article/understanding-consent-under-the-gdpr.

[10] *See* Masooda Bashir, et. al, *Online Privacy and Consent: The Dilemma of Information Asymmetry*, (rel. Nov. 6, 2015), at 2, https://www.asist.org/files/meetings/am15/proceedings/submissions/papers/97paper.pdf.

RISK MANAGEMENT SHOULD REMAIN A CORPORATE, NOT CONSUMER, RESPONSIBILITY

Users should expect organizations to mitigate the risk of harmful use of personal data. This is a reasonable expectation considering the imbalanced relationship between users and organizations. It also provides a new incentive for companies to generate innovative privacy tools that reduce the likelihood of consumer harm. For instance, in the digital space, organizations establish the means and methods to access their products and platforms. Generally speaking, these services are only provided once the user surrenders personalized data to the organization. Users should neither be expected to understand the full extent to which data collection systems and processes work nor are they in a position to take the actions necessary to control privacy outcomes. Thus, putting the onus on consumers to prevent misuse of their personal data would simply be unfair.

Companies are uniquely positioned to manage and mitigate privacy risks. As data sharing models become more sophisticated, mistakes are inevitable and can have far-reaching effects on consumers, especially in communities of color.[11] For people of color with limited resources or opportunity to correct errors, data collection has historically been used to manipulate criminal justice, housing, financial, and health care outcomes to their detriment. Thus, companies should be required to take additional steps to not only safeguard information that is collected, they should also be held accountable for its misuse.

Furthermore, in the event that data is improperly shared, consumers have an immediate right to know and be informed about remedial measures. In an era where technology companies are constantly coming forward to disclose major data breaches, organizations should be required to take additional steps necessary to reduce the harmful use of personal data.

CONSUMERS NEED ACCESS AND OPPORTUNITY TO CORRECT DATA

We generally agree with NTIA's Access and Correction outcome. Communities of color require reasonable, simple, and inexpensive access to their data for the purposes expressed in the RFC. However, we recommend that NTIA clarify its usage of "qualified access." In particular, we are concerned the vague nature of the phrase would ultimately limit which individuals could access their data and what information is available for correction. That said, consumers should be protected from security and fraud risks. Safeguards should be implemented to prevent bad actors from using the process to gather data about third parties.

As stated in the prior section, the consequences of incorrect data can lead to negative implications, especially for communities of color. They include a large population of consumers with the least resources, but the greatest exposure. Too often, these consumers are the last to know when information is improperly shared and the least equipped to correct or delete personal data. Companies should have systems in place that allows consumers to access profiles of personal data and correct or delete information.

[11] *See* Brian Woolfolk, *Don't let internet privacy disputes harm communities of color*, THE HILL, June 9, 2018, https://thehill.com/opinion/civil-rights/393043-dont-let-internet-privacy-disputes-harm-communities-of-color.

THE FEDERAL LANDSCAPE MUST BE HARMONIZED WITH STRONG, CONSISTENT PRIVACY PROTECTIONS

While it is vital for any legislation to be driven by consumer privacy principles of access, fairness, and transparency, ultimately the effects of the legislation must be comprehensible for consumers and enforceable by the body charged to do so. Strong, consistent federal privacy protections will provide consumers with the protections they demand. Users expect to have consistent privacy protections and establishing a strong, enforceable federal framework will improve transparency and make disclosures more effective. Such a framework will undoubtedly make it easier for someone to understand his or her privacy rights, and set the bar for the behavior and norms expected online, regardless of the nature of the consumer's Internet use.

COMPREHENSIVE PRIVACY LEGISLATION SHOULD APPLY TO ALL ENTITIES THAT COLLECT PERSONAL DATA WITHIN THE ONLINE ECOSYSTEM

We agree that comprehensive privacy legislation should apply to all entities that collect personal data within the online ecosystem. This includes both Internet service providers and edge providers. The Federal Trade Commission (FTC) has long-viewed certain categories of data as highly sensitive and a comprehensive framework should provide heightened protections for certain types of data that are considered highly sensitive. These include health information, financial information, geolocation, children's information, and social security numbers.[12] The Federal Communications Commission (FCC) has also found that web-browsing and application usage history can be sensitive.[13] Notably, as technology develops, new consumer harms may be discovered from other categories of data collection. A comprehensive framework should adopt a forward-looking approach that considers new categories of data as highly sensitive.

A comprehensive framework should also prohibit certain harmful uses of data regardless of the entity collecting the data. Companies can use data from race, political opinions, religion, employment, and lending to draw inferences that can negatively impact communities of color -- and have done so in the past. For example, Facebook has consistently faced criticism for enabling advertisers to target certain demographics preventing communities of color from receiving housing ads, including African Americans, Latinos, and Asian Americans.[14] In the 2016 election, the Trump campaign used targeted advertising on Facebook to engage in a campaign to suppress black voters.[15] Data brokers can and do use financial lending information

---

[12] *See Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policy Makers*, Federal Trade Commission (rel. Mar. 2012), at 58-60, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[13] *See Protecting the Privacy of Customers of Broadband and other Telecommunications Services,* Report and Order, 31 FCC Rcd 13911, 13982 para. 181 (rel. Nov. 2, 2016).

[14] *Facebook Sued by Civil Rights Groups for Discrimination in Online Housing Advertisements*, National Fair Housing Alliance (rel. Mar. 27, 2018), https://nationalfairhousing.org/2018/03/27/facebook-sued-by-civil-rights-groups-fordiscrimination-in-online-housing-advertisements/.

[15] *See* Joshua Green and Sasha Issenberg, *Inside the Trump Bunker, With Days to Go*, Bloomberg, Oct. 27, 2016, https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go.

to target communities of color with predatory marketing and lending.[16] This type of data usage is inherently discriminatory and disproportionately impacts communities of color currently, and will continue to do so in the future without additional privacy protections in place. A comprehensive privacy framework must address harmful uses of data and establish standards that prohibit these practices.

ENFORCEMENT MECHANISMS MUST EMPOWER FEDERAL AND STATE AUTHORITIES TO PROTECT CONSUMER PRIVACY

The RFC highlights the FTC as the appropriate agency to enforce consumer privacy. If the FTC is to enforce established privacy rules, the agency must be better equipped with more resources and stronger enforcement authority. Consumers in the digital space rely on consistent and clear enforcement mechanisms to hold organizations accountable to established privacy standards. This is especially true for underserved communities who have neither the means nor the knowledge on what recourse can be taken against organizations who violate established privacy standards. Accordingly, the FTC would need rulemaking authority, the ability to assess civil monetary penalties for violations, and sufficient staff who have the requisite expertise.

It is also essential for federal and state law enforcement authorities to work together to ensure that these challenges are addressed responsibly and effectively. Regulating a digital medium will require enforcement from multiple entry points to ensure a pervasive effect. To this end, state attorneys general must be empowered to enforce privacy laws. Danielle Citron explains other reasons why state attorneys general play an important role in enforcing privacy standards:

> State attorneys general have been nimble privacy enforcement pioneers, a role that for practical and political reasons would be difficult for federal agencies to replicate. Because attorneys general do not have to wrestle with the politics of agency commissioners or deal with layers of bureaucracy, they can move quickly on privacy and data security initiatives. Career staff have developed specialties and expertise growing out of a familiarity with local conditions and constituent concerns. Because attorneys general are on the front lines, they are often the first to learn about and respond to privacy and security violations. Because constituents express concern about privacy and data security, so in turn do state attorneys general who tend to harbor ambitions for higher office.[17]

A STRONG FEDERAL FRAMEWORK REQUIRES INTERAGENCY COOPERATION

Protecting consumer privacy is simply too big for one federal agency to handle on its own. It will require interagency cooperation to ensure strong federal oversight. While the FTC is the agency with general privacy jurisdiction, sector-specific agencies also play a role and have expertise in protecting consumer privacy. The FCC, for example, has decades of experience protecting

---

[16] *See Civil Rights, Big Data, and Our Algorithmic Future: A September 2014 report on social justice and technology*, Upturn (rel. September 2014), at 9, https://bigdata.fairness.io/wp-content/uploads/2015/04/2015-04-20-Civil-Rights-Big-Data-and-Our-Algorithmic-Future-v1.2.pdf.

[17] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747, 750 (2016).

consumer privacy over telecommunications services. Comprehensive privacy legislation should recognize the role of the FTC and other agencies in protecting privacy, and build on their respective experience and expertise overseeing entities subject to sector-specific laws and regulations, such as HIPAA, GLBA and laws that govern telecommunications.

CONCLUSION

The Internet has proven itself to be a transformative tool, but one that can create great harm if not managed properly and to the benefit of those least able to protect their online data. By taking a consumer and civil rights focused approach, we believe that privacy legislation will not only protect consumers online, but facilitate greater participation in the online ecosystem. Those rules should have transparency, clarity, consistency, and strong enforcement mechanisms at its core if we are to ensure that the right to privacy protections in the digital age reaches every individual within every community.

Sincerely,

Asian Americans Advancing Justice-AAJC
Common Cause
National Hispanic Media Coalition
National Urban League
OCA-Asian Pacific American Advocates