Before the
U.S. DEPARTMENT OF COMMERCE,
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, D.C. 20230

In the Matter of	)	
	)	Docket No. 180821780-8780-01
Developing the Administration's	)	
Approach to Consumer Privacy	)	

COMMENTS OF THE NATIONAL COUNCIL OF NEGRO WOMEN, INC.

INTRODUCTION

The National Council of Negro Women, Inc. ("NCNW")[1] respectfully submits these comments in response to the National Telecommunications and Information Administration's ("NTIA") Notice of Request for Public Comments in the above captioned matter.[2]

Given the well-documented history of distrust between Black Americans and institutions intended to serve in their best interests, such as the healthcare industry[3] and the financial services industry,[4] ensuring that personal data is adequately protected is important to renewing consumer trust and to our nation's continued growth and advancement in this digital age. "As seen in data collected by the NTIA, at least a third of online households have been deterred from certain forms of online activity, such as financial transactions, due to privacy and security concerns."[5]

---

[1] The National Council of Negro Women, Inc. ("NCNW") was founded in 1935 by influential educator and activist, Dr. Mary McLeod Bethune. Comprised of more than 200 community-based sections and 30 national women's organizations, NCNW is an organization of organizations. NCNW's mission is to lead, advocate for, and empower women of African descent, their families, and their communities.

[2] *Developing the Administration's Approach to Consumer Privacy*, Department of Commerce, National Telecommunications and Information Administration, Docket No. 180821780-8780-01, Notice of Request for Public Comments, 83 Fed. Reg. 48600, available at https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf (Sep. 26, 2018).

[3] The U.S. Public Health Service (PHS) Syphilis Study, also known as the "Tuskegee Study of Untreated Syphilis in the Negro Male," was intended to record the natural history of syphilis in Blacks. A total of 600 men were enrolled in the study. Researchers ha not informed the men of the actual name of the study, its purpose, and potential consequences of the treatment or non-treatment that they would receive during the study. *Tuskegee University*, "About the USPHS Syphilis Study," https://www.tuskegee.edu/about-us/centers-of-excellence/bioethics-center/about-the-usphs-syphilis-study.

[4] After the creation of the Freedman's Bank by President Abraham Lincoln's signing of the Freedman's Bank Act in 1865, recently emancipated Black Americans had their first monies as freed persons mishandled. Black wealth issues are historically rooted in a persistent pattern of loss and mistreatment of their finances, the beginning of such mishandling being documented during Reconstruction. Marcus Anthony Hunter, "Black America's distrust of banks rooted in Reconstruction," The Chicago Reporter (Feb. 22, 2018), https://www.chicagoreporter.com/black-americas-distrust-of-banks-rooted-in-reconstruction/.

[5] *Developing the Administration's Approach to Consumer Privacy*, *supra* note 2 at 48600.

Thus, renewing trust and ensuring adequate data protection is an issue important to all Americans, no matter their race.

If gone unregulated, the inefficacy of privacy protections will affect the ability of all Americans to safely use the Internet and to enjoy the benefits, such as telehealth and online banking, which excitingly come with the continued growth of our digital landscape.

With a programmatic platform of "Four for the Future," NCNW actively advocates on issues, such as educating its membership on health concerns, like HIV/AIDS, which impact the African American community and promoting economic empowerment through financial literacy and short- and long-term financial planning. Universal access to innovative technologies like telehealth and online banking are aptly positioned to play a pivotal role in our future discussions on health education and economic independence. Thus, the NTIA's proposed privacy outcomes and high-level goals directly impact NCNW's membership and NCNW's ability to continue to effectively advocate on their behalf.

Therefore, NCNW offers comments to ensure that NTIA's user-centric privacy outcomes and its high-level goals for federal action accurately address the concerns of communities of color and low-income consumers. Based on NCNW's extensive experience in promoting public policy agendas that advocate for women of African descent, their families, and their communities, NCNW recommends that the following concerns be taken under consideration:

A. **Transparency.** Mandating notice and choice is not the issue. Long, legal, regulatory-focused privacy policies are. Thus, companies that collect consumers' data should continue to provide each consumer with knowledge, notice, and the option to say "no." However, to achieve this transparency outcome, this information should be displayed using plain language and include the option for consumers to access such information in languages other than standard U.S. English. Such transparency creates an atmosphere of trust between the consumer and the company.
B. **Control/Access and Correction.** While a user should have reasonable control over the collection, use, storage, and disclosure of its non-sensitive personal information, consumers should have *complete* control over a company's collection, use, storage, and disclosure of any sensitive data pertaining to their unique digital persona. This entails the right to access, modify, and delete the digital data that companies have collected. Consumers should also have the option to opt-in to a company's use of their sensitive data, including its sale to third parties, with exceptions for use and disclosure as necessary to provide the service and implement reasonable security safeguards.
C. **Accountability.**[6] The Federal Trade Commission ("FTC") should continue as the federal consumer privacy enforcement agency. However, changes should be made with regard to the FTC's resources, processes, and statutory authority in order to allow for sufficient

[6] This section also addresses the NTIA's high-level goals of harmonizing the regulatory landscape, comprehensive application, FTC enforcement, and scalability.

review of consumer data privacy complaints and for the agency's ability to impose fines for data breaches.

I. TRUST THROUGH TRANSPARENCY

"Trust is at the core of the United States' privacy policy formation."[7] Accordingly, trust should also be at the core of the privacy policy formation for any company operating within the U.S. Thus, companies should move from the stance of asking consumers for forgiveness to the stance of asking consumers for permission. NCNW agrees that the consent of an informed user is the end goal. Thus, in the creation of a truly transparent landscape, a company should make the request for the use of a consumer's personal data using plain language. "Plain language (also called plain writing or plain English) is communication [that an] audience can understand the first time [that] they read or hear it."[8]

Although most people in the United States speak English and most governmental functions are in English, a 2015 U.S. Census Bureau report revealed that at least 350 languages are spoken in American homes.[9] Furthermore, many variations of African Diasporic speech and language, including French Creole, Yoruba, and Swahili, are spoken throughout the world and, more relevantly, within the borders of our own nation. Ultimately, "[o]ur efforts to develop a just society must include critical examination of our attitudes toward speech and language, as well as commitment to addressing linguistic barriers…"[10] Thus, the privacy disclosures that companies make to consumers should not only be clear and concise, but also be made available in multiple languages, which can be achieved by creating webpages that are readable by translation software, in order to adequately address the linguistic diversity of our country.

II. COMPLETE CONSUMER CONTROL

Data is power in the digital economy.[11] Thus, "he who owns the data [and] who makes decisions on who has access to what based on that data, holds the power."[12] As such, consumers should

---

[7] *Developing the Administration's Approach to Consumer Privacy*, 83 Fed. Reg. at 48600.

[8] "What is plain language?" (2018) https://www.plainlanguage.gov/about/definitions/. The Plain Writing Act of 2010 defines plain language as "writing that is clear, concise, well-organized, and follows other best practices appropriate to the subject or field and intended audience." (124 STAT. 2861, §3(3)).

[9] U.S. Census Bureau. (2015, Nov. 3). Census Bureau Reports at Least 350 Languages Spoken in U.S. Homes (Report No. CB15-185). Retrieved from https://www.census.gov/newsroom/press-releases/2015/cb15-185.html. See also, Juan Castillo, "At Least 350 Languages Spoken In US Homes: New Report," NBC News (Nov. 4, 2015), https://www.cnbc.com/2015/11/04/at-least-350-languages-spoken-in-us-homes-new-report.html.

[10] Audrey P. Watkins, "Negotiating Speech and Language in the African Diaspora: Politics of Linguistic Diversity," International Journal of Whole Schooling (Vol. 4, No. 2), p.4.

[11] Bernard Marr, "Where Can You Buy Big Data? Here Are The Biggest Consumer Data Brokers," Forbes (Sep. 7, 2017), https://www.forbes.com/sites/bernardmarr/2017/09/07/where-can-you-buy-big-data-here-are-the-biggest-consumer-data-brokers/#65b45cb46c27.

[12] Angelique Carson, International Association of Privacy Professionals, April 13, 2006; https://iapp.org/news/a/when-surveillance-perpetuates-institutional-racism/ (accessed on October 8, 2018).

have reasonable control over how their personally identifiable information is used, distributed, and monetized by the companies to which they entrust such information. This can be achieved by requiring informed consent through clear opt-in/opt-out controls and by offering consumers fair value in return for a company's sale of their sensitive personal information, particularly if the selling of the consumer's information is not necessary to provide the service or to implement reasonable security safeguards.

When further constructing these approaches, the European Union's General Data Protection Regulation ("GDPR")[13] serves as a model for how to ensure consumer rights are practically protected. Although the GDPR allows companies the right to use a consumer's information without consent in order to provide requested products or services, for legal compliance reasons, or for legitimate business purposes,[14] the GDPR is a champion for consumer consent at its core. In addition to express consent requirements, the data privacy regulation gives consumers the right to access, correct or delete, and port their personal data from one company to a new provider. This standard of consumer control over data collection, correction, deletion, and portability should also be afforded to U.S. consumers.

According to the GDPR, "personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[15]

NCNW agrees with the GDPR's definition of personal data, adding that sensitive data also includes any data that reveals:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person; and
- Data concerning health or a natural person's sex life and/or sexual orientation.[16]

Knowing that within the past five years, companies, such as Facebook,[17] JP Morgan Chase, Yahoo, and eBay,[18] have been, and continue to be, victims of data breaches, companies should

---

[13] The GDPR is arguably the biggest change to the regulatory landscape of data privacy. See, EUGDPR.org, https://eugdpr.org/the-regulation/.

[14] General Data Protection Regulation (GDPR). (2018). *General Data Protection Regulation (GDPR),* Article 6(1)(a)-(f). Available at: https://gdpr-info.eu/art-6-gdpr/.

[15] Id. at Article 4(1). Available at: https://gdpr-info.eu/art-4-gdpr/.

[16] GDPR, *supra* note 14, at Article 9, paragraph 1. Available at: https://gdpr-info.eu/art-9-gdpr/.

provide conspicuous consent options for consumers to opt-in to a company's use of their sensitive data. Having opt-in and opt-out capabilities based on the sensitivity and use of the data strikes a fair balance between a company's flexibility to innovate and to manage compliance costs and a consumer's fundamental right to privacy and its control over the use of its data.

III. CORPORATE CULPABILITY

With many states enacting their own privacy laws,[18] NCNW recognizes the practical need for federal preemption on privacy regulation in order to avoid consumer confusion. Thus, to promote legal clarity and to harmonize the regulatory landscape, NCNW agrees with the NTIA that "the FTC is the appropriate federal agency to enforce consumer privacy with certain exceptions made for sectoral laws outside the FTC's jurisdiction, such as HIPAA."[19] NCNW is also of the position that the FTC should continue to operate under its longstanding case-by-case adjudicatory approach, rather than adopting prescriptive rules through a rulemaking process. Furthermore, in following the GDPR's standard, privacy decisions made by the FTC should apply to all companies, controllers and processers, which process the personal data of consumers who reside in the United States, regardless of the company's location and regardless of whether the processing takes place in the U.S. or not.[20]

In the absence of a joint effort of "a public-private partnership to lay out voluntary privacy best practices,"[21] the enactment of privacy legislation should be left to Congress. However, until such public-private partnerships materialize or until congressional legislation is promulgated, the FTC is the only line of defense for ensuring consumer protection. Therefore, there must be a clear national standard that will allow the FTC to serve as a strong enforcement mechanism that produces individualized resolutions regarding consumers' privacy concerns.

Currently, the FTC's Bureau of Consumer Protection takes complaints concerning how a company is handling a consumer's personal information.[22] Although "[t]he FTC encourages

---

Need to Know as Fallout Widens," NY Times (Mar. 19, 2018) https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

[17] Taylor Armerding, "The 17 biggest data breaches of the 21st century," CSO (Jan. 26, 2018), https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

[18] Several states, including California, Delaware, and Nebraska, have promulgated legislation on a variety of issues regarding consumer privacy and data security, such as data disclosures, conspicuous privacy policies, and explicit opt-in requirements. National Conference of State Legislatures, "State Law Related to Internet Privacy," (Sep. 24, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

[19] *Developing the Administration's Approach to Consumer Privacy*, 83 Fed. Reg. at 48602.

[20] EUGDPR.org, *supra* note 13.

[21] Shannon Vavra, Kim Hart, and David McCabe, "Scoop: The White House looks to coordinate online privacy plan," Axios (June 20, 2018), https://www.axios.com/scoop-the-white-house-looks-to-coordinate-online-privacy-plan-a51691cf-78d9-466e-8deb-27a66b1843c7.html.

[22] See Federal Trade Commission, FTC Complaint Assistant, available at https://www.ftccomplaintassistant.gov/#crnt.

consumers to file a complaint whenever they have been the victim of fraud, identity theft, or other unfair or deceptive business practices…filing a complaint will not guarantee that their problem will be fixed."[23] Thus, it is crucial that changes are made to the FTC's resources, processes, and statutory authority in order for the FTC to have strong enforcement capabilities that will allow for the sufficient review of consumer data privacy complaints, the authority to investigate these complaints, and the ability to remedy such harm, including to impose fines for data breaches.

Ultimately, "[f]ederal law is enforced through a combination of public and private efforts."[24] Therefore, it is essential for federal and state law enforcement authorities to work together to ensure that consumer data privacy concerns are addressed responsibly and effectively. Specifically, state attorneys general must be empowered to enforce privacy laws. Such enforcement authority ultimately provides the "policy benefits of decentralized decision making" that can be adapted to local conditions and local tastes.[25] Thus, for maximum consumer protection, strong state enforcement authority will ensure that federal law adequately addresses the consumer privacy concerns of a state's constituents and that, in cases where the FTC chooses not to adjudicate a consumer's complaint, non-complying companies are held accountable for inadequate data security.

Lastly, NCNW would like to commend the NTIA for explicitly taking into consideration the importance of strong consumer privacy outcomes being deployed in proportion to the scale and scope of the information an organization is handling, so as to not adversely affect small businesses. With a significant number of our membership being small business owners or actively pursuing entrepreneurial endeavors, NCNW is mindful of the often deleterious effects that staunch regulatory frameworks can have on small and minority-owned business and we are glad to see that the NTIA recognizes the same.

CONCLUSION

NCNW is aware of the importance of maintaining a competitive broadband and communications marketplace in providing digital services to the greatest number of people. Thus, NCNW's comment in no way intends to impede a company's ability to contribute to the innovation of the digital landscape. However, in order for any marketplace to thrive, there must be a foundation of trusting consumers at its base. Thus, implementing consumer privacy outcomes and clear privacy compliance standards that address the issues of the largest cross section of people is paramount.

As advocates for women of African descent, NCNW requests that the NTIA encourage that further data collection be conducted in order to analyze the potential peripheral effects of these proposals on minority women, their families, and their communities. The proposed rules should

---

[23] Federal Trade Commission, Filing a Complaint, available at https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/filing-complaint.

[24] Margaret H. Lemos, *State Enforcement of Federal Law*, 86 NYU Law Rev. 698 (2011).

[25] Id. at 750.

As advocates for women of African descent, NCNW requests that the NTIA encourage that further data collection be conducted in order to analyze the potential peripheral effects of these proposals on minority women, their families, and their communities. The proposed rules should ensure that all consumers, including those from marginalized and low-income populations, are able to protect, access, and control the use of their personal information in this 21st century digital market.

Respectfully Submitted,

/s/ Janice L. Mathis

Janice L. Mathis, Esq.
Executive Director
National Council of Negro Women, Inc.
633 Pennsylvania Ave. NW
Washington, D.C. 20004
(202)737-0120

November 8, 2018