To: United States Department of Commerce, NTIA
From: Emily Ross
Re: Docket No. 180821780– 8780–01—Request for Comments on Developing the Administration's Approach to Consumer Privacy
Date: October 28, 2018

M E M O R A N D U M

I. Overview

The Trump Administration's explicit goals for improving consumer data privacy in the U.S. highlights the urgent need for a federal regulatory scheme. More than ever, consumers seek reliability and security in the online entities that they are using. Furthermore, federal regulation is the only approach that will adequately accommodate the landscape of data collection, as it permeates interstate commerce and extends across state lines, thereby creating a constitutional necessity to have federal regulation.[1]

Historically, the United States has taken a business-minded approach to federal consumer regulations.[2] Our laissez-faire economic practices have allowed corporations to freely operate in online markets prior to the widespread use of the internet.[3] This approach has continued with the growth of technology and use of the internet, creating fundamental problems with current self-regulated data collection practices. Previous attempts to utilize privacy torts in consumer privacy have failed.[4] Therefore, there is a need for comprehensive federal regulation to combat the lack of legal remedies for consumer data privacy practices that infringe on the right to privacy.

[1] *See generally* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELATIONS (last updated Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.
[2] Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 23-25 (2000).
[3] *See* Shaffer *supra* note 2.
[4] Daniel J Solove & Woodrow Hartzog, *The FTC and The New Common Law of Privacy*, 114 COLUM. L. REV. 583, 590-591.

II. Implementing a Regulatory Scheme Mirroring the Rights Established in the General Data Protection Regulation

With globalization and the increase of international economic markets, it is in the best interest of the U.S. to take a similar approach to consumer data collection that the European Union has implemented.[5] In May 2018, the EU instituted the General Data Protection Regulation ("GDPR").[6] This wide-spread and stringent regulation led U.S.-based corporations to question what accommodations were necessary in order to comply with the regulation.[7] The jurisdictional element of the GDPR extends to all citizens of the EU, regardless as to whether corporations are based in other countries.[8] Therefore, with the goal of corporate uniformity and human rights, it is in the best interest of the U.S. to comply with international standards to establish themselves as leading in data compliance.

Ultimately, the best approach the U.S. can take is to mirror the rights and procedures set forth in the GDPR, both to ensure the best protections for consumers and to ensure U.S. corporations are abiding by international standards.

a. Goals Set Forth by the Administration

The goals set forth by the Trump Administration are to prioritize transparency, individual control, reasonable minimization of data, security, access and correction of data, risk management by organizations, and accountability. In transforming these broad goals into an

[5] *See generally* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 23-25 (2000).
[6] *See generally* Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119/1 [hereinafter GDPR].
[7] *See generally* Jeff John Roberts, *The GDPR Is In Effect: Should US Companies be Afraid?*, FORTUNE (May 25, 2018), http://fortune.com/2018/05/24/the-gdpr-is-in-effect-should-u-s-companies-be-afraid/.
[8] Kurt Wimmer, *Free Expression and EU Privacy Regulation: Can the GDPR Reach US Publishers?*, 68 SYRACUSE L. REV. 547, 560-61 (2018).

implementable regulatory scheme, the administration must keep in mind a rights-based approach when structuring the text of the regulation.

While currently, the U.S. enforces a permissive approach to data collection, or by default allowing the collection of user data; the new regulation should be more restrictive and view privacy as an individual right, or by default preventing the collection of data.[9] Viewing data-protection as a human right, rather than permissive practices by corporate entities, is an essential requirement for the new U.S. regulation.

III. Improvements

In this comment, I will detail two points of improvement for the Administration's regulatory goals: improvements to "notice and choice" and instituting "privacy-by-design".

a. Notice and Choice

First, improvements to current "notice and choice" regime should encompass purpose minimization and data minimization. Notice and choice operates on the presumption that consumers are willingly choosing to convey their personal information to data collectors after they are given adequate notice that their data will be collected and for what purposes it will be used.[10] This begs the question as to what should be considered adequate "notice" under new U.S. regulations; as currently, "notice and choice" is autonomously regulated by corporate entities.[11]

Currently, "notice" for data collection comes in the form of terms and conditions, privacy policies, and cookie collection. All of these, as currently used, are often not easily accessed by consumers or appear after the consumer has already entered their personal data. Most notorious

[9] *See generally* WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 257 (Robert C. Clark et al. eds. 2016) (detailing the permissive and restrictive approaches to data protection).
[10] *See* Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74, 77 (2018).
[11] *See generally* Corrie Faith Cranor et al., *A Journal of Law and Police for the Information Society: Are they Worth Reading? An In-Depth Anaylsis of Online Trackers' Privacy Policies*, 11 ISJLP 325 (2015) (discussing the issues with self-regulation in corporate data privacy "notice and choice" regime and posing potential solutions to increase online tracking transparency).

are "Agree to Terms" that require checking a box to proceed with online usage. This form of notice is insufficient choice for individuals, as there is a lack of realistically comprehendible information and no way to opt out of the unilateral terms of agreement.[12]

Furthermore, current frameworks being utilized for "notice and choice" disclosures are incredibly difficult to read and comprehend, even for a user who is actively seeking them out.[13] Disclosures are drafted in an abnormally small font and filled with legal jargon.[14] This style indicates that privacy policies have not been drafted for the goals of readability, comprehension and easy access. Furthermore, some would argue that the interface and design tactics employed by data collectors are used with the intention of misleading or misinforming consumers.[15] With such a lack of understanding, it is hard to believe that consumers are being "put on notice" and "consenting" to the future use of their information.[16]

With the proliferation of corporations operating online, a consumer's inability to proceed without "agreeing to the terms" provides no choice for the consumer and allows corporations to dictate how and what they will use individuals' data for.[17] Most often, if a consumer chooses not to consent to the practices, they are unable to proceed with the uses of the website. This effectively discriminates against individuals who are concerned with the practices of data collection and desire to keep their private information from being collected or sold.

---

[12] *See* Robert H. Sloan and Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370, 390 (2014).
[13] *See generally* Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74, 81-84 (2018).
[14] *See* Joel R. Reidenberg, Stanley D. and Nikki Waxberg, *Privacy Harms and the Effectiveness of Notice and Choice Framework*, 11 ISJLP 485, 490-92 (2015).
[15] *See* Reidenberg *supra* note 14.
[16] Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74, 116 (2018) ("[P]olicy designs can also mislead the general public into making risky privacy decisions they would have otherwise opted against").
[17] *See* Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 322-23 (2013).

Therefore, the U.S. can improve their "notice and choice" regime by including stricter notice and consent requirements, allowing individuals to "opt-in" to data collection rather than have data collection as a default. Through a consumer-focused approach to "choice", consumers actively chose what disclosures they permit, and "opt-in" to data collection.[18] Through increased autonomy of consumers, there will be an increased confidence with any disclosures of personal data. Furthermore, with strict consent regulations, users will be able to opt out of having data collected and stored more frequently than the current "notice and choice" regime.[19] This opting out will lead to increased data minimization by parties as they will be forced not to collect and store data when consumers opt out of specific collections.

Through adopting consumer-based "notice and choice" requirements, the U.S. will also move towards the goals stated by the Administration— reasonable data minimization. Through the GDPR, the EU will see more uniformity in data collection practices requiring explicit notice as to what information is being collected and for what purposes. The U.S. should adopt laws that, by default, prevents the collection of data and lists exceptions to that default rule.[20] Through this approach to data collection, industry standards would move towards data minimization, as data collections would be prevented except for the explicit permitted scenarios.[21] This practice focuses on restricting data collection to what is absolutely necessary for the functionality of the data-collecting entity. Thereby, creating incentives for data collectors to minimize the amount of data that is being collected, if regulations restrict the collection to only what is necessary.

---

[18] *See* Joseph A. Tomain, *Online Privacy & The First Amendment: An Opt-In Approach to Data Processing*, 83 U. CIN. L. REV. 1, 4–6 (2014).
[19] *See* Tomain *supra* note 18.
[20] *See generally* GDPR Art. 6.
[21] *See generally* The Sedona Conference, *The Sedona Conference Practical In-House Approaches for Cross-Border Discover & Data Protectio*n, 17 SEDONA CONF. J. 397 (2016).

Furthermore, data-minimization leads to lower costs and risks associated with data protection, as entities possess less sensitive information that the need to encrypt and protect.[22]

In addition to data minimization, improvements to "notice and choice" should also include purpose minimization, or explicitly stating the purpose of the data collection and any collection outside the explicit purpose will require additional consent. Purpose minimization will allow individuals to be informed as to the purpose and uses of any data collection. Purpose minimization contributes to overall goals of data minimization, in that data collection will be limited to the consent of consumers based on a purpose of use.[23] Thereby, limiting data collection only for specific and explicit purposes.[24]

Through improving "notice and choice" standards, the U.S. will allow consumers to actually be informed regarding the information that is collected and empower them to choose to opt out if they do not wish for such information to be collected.[25] Viewing "notice and choice" as a measure to protect individuals from the onset rather than after information is gathered encourages entities to design their notices in a way that alerts the consumer as to what is being collected and for what purpose in a more comprehendible and explicit manor.

For the foregoing reasons, I would strongly urge the Administration to revise their priorities of "notice and choice" to include measures of data minimization and purpose minimization. In viewing data collection as passive rather than active, consumers inherently lack the control and choice as to what data is being collected and monitored.[26] Through improving "notice and

[22] *See* Birnhack et al., *Privacy Mindset, Technological Mindset*, 55 JURIMETRICS J. 55, 97–98 (2014).
[23] *See* Birnhack et al., *supra* note 22 at 2019.
[24] *See* Birnhack et al., *supra* note 22 at 2019.
[25] *See* Ari Ezra Waldman, *Designing Without Privacy*, 55 Hous. L. Rev. 659, 669 ("As a theoretical matter, the notion of the autonomous user is a myth").
[26] *See generally* WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 328 (Robert C. Clark et al. eds. 2016) (discussing the methods employed for active and passive data collection).

choice", data collection will be an active regulation that proactively encourages consumers to exercise control over their personal information.

b. Privacy-by-Design

Second, the Administration should add "privacy-by-design" to their goals. "Privacy-by-design" is the concept that privacy should be instituted in the ground-up design of entities online; and that, by design, data collectors should prioritize privacy.[27] Predominantly in the U.S., organizations do not prioritize privacy in the design of their internet access to consumers, but rather attempt to implement some form of patchwork privacy after the initialization of the data collection.[28] Therefore, by including privacy frameworks from the ground-up design, there will be more holistic approach and better practices in place to ensure the protection of personal information.

The GDPR institutes a similar requirement of "privacy-by-design" or "privacy-by-default" in their regulatory requirements for data collectors.[29] The regulation includes business processes that handle personal data must be designed and built with consideration of the principles to safeguard data; thereby making privacy default to the design process. Two examples of privacy built into the design of data collection, that should be adopted in the U.S. regulation, are pseudonuymization and anonymization of any data that is collected.[30]

With the use of pseudonuymization, or de-identification, in the collection and storing of data, personally identifiable information will decreasingly be connected and associated with a specific

[27] ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE, 85-90 (2018); Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L. J. 1333, 1335 (2013).
[28] *See generally* Rubenstein et al. *supra* note 27.
[29] *See* GDPR Art. 25.
[30] Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L. J. 1333, 1357 (2013) (discussing encrypting and use of pseudonyms in privacy engineering).

individual.[31] Furthermore, in the case of data breaches, the use of pseudonyms can allow individuals to be assured that their sensitive information will be somewhat protected, or at least not overtly traceable to a specific individual.[32] Currently, data breaches are proliferating. Furthermore, data breaches lead individuals to worry about how their personally identifiable information is being secured by entities. From Equafax[33] to Ashley Madison[34], the use of pseudonyms can decrease the harm that occurs when data is collected and not secured.

Another feature of "privacy-by-design" is the full anonymization of data that is collected, meaning full and specific encryption of all data collected as to ensure heightened security standards.[35] By encrypting data, any identifiable information that is analyzed would be encrypted to minimize likability with a particular individual. Furthermore, with specific encryptions, it is increasingly difficult for information to be released or misused by any third-party. Through the decreased ability of third-party access to data, consumers will feel more secure with entities that possess any of their personally identifiable information.

The regulatory requirement of "privacy-by-design" should effectively lead to data minimization and data avoidance. With "privacy-by-design", the best way to secure data from the initial collection is to minimize the amount of data that a specific entity holds.[36] Furthermore, there will be a general reduction of privacy concerns with less data being collected, thereby ensuring that consumers feel comfortable with disclosing personal information. Through hiring

---

[31] Cedric Burton & Sara Hoffman, *Personal Data, Anonymization, and Pseudonymization in the EU*, WSGR DATA ADVISOR (last updated Sep. 15, 2015), https://www.wsgrdataadvisor.com/2015/09/personal-data-anonymization-and-pseudonymization-in-the-eu/.
[32] *See generally* Burton et al. *supra* note 31.
[33] *See generally The Equifax Data Breach*, FEDERAL TRADE COMMISSION (last visited Oct. 18, 2018), https://www.ftc.gov/equifax-data-breach.
[34] *See generally* Robert Hackett, *What to Know About the Ashley Madison Hack*, FORTUNE (last updated Aug. 26, 2015), http://fortune.com/2015/08/26/ashley-madison-hack/.
[35] *See* Hackett *supra* note 34.
[36] Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L. J. 1333, 1357-58 (2013).

privacy professionals, "privacy-by-design" can be a continued practice and norm in the corporate setting. Subsequently, when consumers are conscious that corporations are working to instill privacy in the corporate ethos and protect their users, then consumers feel more confident in corporate entities handling what information they do have. By instituting "privacy-by-design", entities are forced to think of data privacy as an essential element of operating online.

Ultimately, "privacy-by-design" creates holistic approach to privacy protection while requiring corporate entities to instill new ethos to organizational practices to ensure privacy is prioritized.[37] "Privacy-by-design" can transform how privacy is viewed by data collectors from the beginning, rather than attempting to instill patchwork privacy practices after the product is being used by the consumer. As privacy is a major concern with consumers, it should follow that privacy is a major concern of corporations.

IV. Policing the New Regulatory Scheme

The most effective way to police a new regulatory scheme would be to have the Department of Justice ("DOJ") as the enforcement agency. Compared to administrative actions currently being taken by the Federal Trade Commission ("FTC"), stronger enforcement is necessary to adequately police a new federal regulation.

There are major problems with FTC enforcement that would be resolved with DOJ enforcement. The FTC provides investigations that are not as transparent and accessible to the public as the judicial process would be. As discussed in *The FTC and the New Common Law of Privacy*, there is little U.S. common law on consumer data privacy due to the FTC

[37] *See* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE, 85-90 (2018)(discussing the significant organizational impact that privacy-by-design has on leading to increased data privacy).

enforcement.[38] And while the FTC seemingly settles a majority of cases in settlement and contractual agreements, the FTC has, through their 15 years of enforcing consumer privacy law, developed substantive methods and norms in data collection.[39] This idea, that an executive-appointed government agency is determining the substantive norms guiding consumer data privacy is anti-democratic and devalues the Constitutional significance of the judicial system. Consumer data privacy is a substantive body of law, with issues of human rights, that should be litigated and decided through the judicial process, thereby increasing the transparency for individuals to know their substantive rights.[40] Having an executive agency determine nearly all outcomes from organizational violations of privacy regulations provides for no judicial check, lack of transparency, and inconsistent outcomes. Therefore, it is important that the new regulatory scheme be enforced by the DOJ to ensure the judicial review of substantive legal issues in consumer data privacy.

Furthermore, the approach to consumer data privacy should put consumer interests above the interests of corporations to ensure the best practices.[41] Therefore, having the DOJ as the enforcement agency would increase investigative abilities and shift focus from normative business practices to the outcomes experienced by consumers. Under the current regime, the FTC approaches privacy problems as "possible flaws in the character of a commercial relationship between a company and an individual;" however, to ensure federal data privacy

[38] Daniel J Solove & Woodrow Hartzog, *The FTC and The New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585–587.
[39] *See* Solove et al. *supra* note 38.
[40] *See generally* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 36-38 (2000).
[41] *See generally* Robert Gellman, *Can Consumers Trust the FTC to Protect Their Privacy?*, AMERICAN CIVIL LIBERTIES UNION (last updated Oct. 25, 2016) https://www.aclu.org/blog/privacy-technology/internet-privacy/can-consumers-trust-ftc-protect-their-privacy (discussing the weaknesses with FTC enforcement of data privacy, however, this article argues the FCC is more apt to enforce data protection laws).

regulations and rights, the best approach is to assume privacy as a human right and have enforcement from the DOJ.[42]

Additionally, the U.S. needs to establish firm penalties if entities violate the new federal regulation.[43] Currently, pursuant to Section 5 of the FTC Act, the FTC does not, on its own, have the power to impose monetary penalties on corporations who violate privacy regulations. In the GDPR, any corporate entity in violation of the rights set forth in the regulation faces a 2% penalty from the corporate revenue or up to $10 million.[44] This staggering penalty provides corporations with coercive incentive to prioritize consumers when structuring their data privacy and data collection practices. Therefore, the most effective way that the U.S. will enforce their new consumer data-privacy regulation will be to have proportional penalties rather than a small flat rate for any violations. Thereby, preventing corporations from violating the regulation in viewing potential penalties as a cost-of-business.

Ultimately, the U.S. regulation should include the DOJ as the enforcement agency with proportional and clear penalties that pose a threat to corporations if they violate the regulatory standard of data privacy practices.

V. Conclusion

Consumer data-privacy is a prevalent issue for individual rights due to the increase of personally identifiable information that is currently collected and stored. It is naïve to believe that individuals can go without disclosing information online, as it has become unavoidable. The

[42] WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 257 (Robert C. Clark et al. eds. 2016).
[43] *See generally* Robert Gellman, *Can Consumers Trust the FTC to Protect Their Privacy?*, AMERICAN CIVIL LIBERTIES UNION (last updated Oct. 25, 2016) https://www.aclu.org/blog/privacy-technology/internet-privacy/can-consumers-trust-ftc-protect-their-privacy (discussing the weak authority and standards of the FTC).
[44] Bernard Marr, *GDPR: The Biggest Data Breaches and the Shocking Fines (That Would Have Been)*, FORBES (last updated June 11, 2018) https://www.forbes.com/sites/bernardmarr/2018/06/11/gdpr-the-biggest-data-breaches-and-the-shocking-fines-that-would-have-been/#2095c35c6c10 (reviewing major data breaches and how the GDPR would have fined those corporate entities); GDPR Art. 83.

internet is now where individuals pay rent, shop, date, receive medical advice, secure employment, and more. Furthermore, with all of this sensitive data being collected, consumers look to the government to protect and police entities that hold their identifiable information.

It is in the best interest of the Trump Administration to make accommodations to their proposed goals that mirror the GDPR, both for human rights and for international business practices. By including stringent "notice and choice" requirements as well as requiring "privacy-by-design," the new U.S. regulation will ensure that consumers are prioritized throughout the process of data collection. Furthermore, the policing of these new regulations is best suited for the DOJ, rather than the FTC, to ensure consumer faith and remain transparent.

Ultimately, if these accommodations are adopted into federal regulation, there will be increased confidence among consumers that their data and private information will be protected in the hands of U.S. entities.