WORLD **PRIVACY** FORUM

Comments of the World Privacy Forum
to the Federal Trade Commission

Regarding Competition and Consumer Protection in the 21st Century Hearings,
Project Number P181201

Via online comment

Federal Trade Commission
Office of the Secretary
Constitution Center
400 7th Street, SW
5th Floor, Suite 5610 (Annex C)
Washington, DC 20024

August 20, 2018

Dear Secretary,

Thank you for the opportunity to comment on the FTC's Hearings on Competition and Consumer Protection in the 21st Century. The World Privacy Forum is a non-profit public interest research group that focuses on data privacy issues, including those relating to technology, health, biometrics, and other topics. Our research, testimony, consumer education, and other materials are available on our webpage, www.worldprivacyforum.org.

In these comments, we are responding to questions 1, 4, 5, 10, 11 and their subparts. We have noted each question and subpart in the headings below. Because some of our comments are cross-referenced, we are uploading these comments in their entirety to each submission category on the FTC website.

1. e. The advisory and advocacy role of the FTC regarding enforcement efforts by competition and consumer protection agencies outside the United States, when such efforts have a direct effect on important U.S. interests

The FTC has acted in an important advisory and advocacy role outside of the US regarding enforcement efforts by consumer protection agencies for many years,

particularly since first the Privacy Shield, and subsequently the EU-US Safe Harbor agreement were negotiated. Now that the EU General Data Protection Regulation (GDPR)[1] is in force, the FTC's role has become even more crucial.

Regarding the EU-US Privacy Shield, the FTC has promised to "give priority" to Privacy Shield referrals and to other Privacy Shield matters as part of agreements and negotiations with Europe regarding consumer privacy.[2] This creates significant procedural and operational burdens, which we suspect have only increased since GDPR came into force.

For example, if European consumers file Privacy Shield complaints in large numbers, what does that mean for Europeans? What does that mean for Americans? What does this mean for the FTC's work load? Does the FTC have funding to increase capacity to handle an increased complaint volume? If no extra funding is made available to the FTC, would American consumers find the FTC to be less responsive to their privacy and consumer protection needs due to personnel shortages?

It is readily demonstrable that it is in the interest of the US to have some form of agreement in place for data transfers between Europe and the US. In an ideal world, if there were torrents of EU complaints, the FTC would get additional funding to meet all of the new demands. And in an ideal world, the FTC would get additional funding to task a team to interface with Europe regarding emerging GDPR issues.

4. [*re: Big Data*] f. Competition and consumer protection implications of use and location tracking mechanisms.

Geolocation is a complex topic. Here, we are making three brief points.

First, it has become extremely difficult for an average consumer to parse location information settings, and company disclosures are not always apace with the need for clearly stated information and easy, centralized controls. See for example the recent Associated Press investigation that found that some of Google's geolocation apps were

---

[1] EU General Data Protection Regulaton, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001R0045&from=EN.

[2] Letter From Chairwoman Edith Ramirez To Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, Describing Federal Trade Commission Enforcement of the New EU-U.S. Privacy Shield Framework, US Federal Trade Commission, July 7, 2016. "Although the FTC does not resolve or mediate individual consumer complaints, the FTC affirms that it will prioritize Privacy Shield referrals from EU DPAs." p. 7. Available at: https://www.ftc.gov/system/files/documents/public_statements/972913/2016-07-06_final_ftc_letter_final_dated_77.pdf. *See also* Privacy Shield Documents, US Department of Commerce, February 23, 2016, https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf.

still collecting geolocation information even after users had paused geolocation collection via the Google "location history" setting for mobile devices.[3] The confusion came with disclosure language that stated "With Location History off, the places you go are no longer stored." (This language has since been edited and improved.)

Geolocation tracking can have multiple levels of controls, including device-level controls, which are separate from controls within the various apps that might be asking to track data. Consumers need to be aware of device-level controls, for example, iOS device controls for geolocation or Android device controls, as well as a wide variety of in-app controls, which may themselves have several layers. This creates the need both for exceptionally clear disclosures, for consumer education, and for consistency of disclosures amongst a wide variety of non-related businesses that utilize geolocation features. The FTC is in a position to be of assistance in creating standards for consistency of disclosures across platforms, operating systems, apps, and dapps[4] that track geolocation.

Second, even aggregate geolocation data, or so-called "big data" geolocation applications may create privacy and security challenges. An example of this can been seen via a data visualization the fitness app Strava released in November 2017 of its users, called the Global Heat Map.[5] The visualization was a heat map which indicated more than 700 million users' fitness activity by geolocation. When the map was viewed at close ranges via the Strava site, the map charted the cycling and running trails of individual Strava users. When members of the US military became aware that service members' jogging or cycling routes on military bases were being made visible, including advance bases overseas, it became a significant press story.[6] The military created refined guidelines for service members who were using Strava. The Strava app did in fact have a privacy setting that allowed for an opt out of heatmap posting, but this situation illustrates how easy it is to simply use a product without knowing all of the precise privacy settings that could be important.

Third, WPF has worked now for nearly twenty years with survivors of crime, including domestic violence and other crimes, to help educate survivors about ways they can improve their everyday privacy practices. Very frequently, location information is a significant safety issue for this group of individuals. The solutions that help these

---

[3] Ryan Nakashima, Google tracks your movements, like it or not, Associated Press. August 13, 2018. https://apnews.com/828aefab64d4411bac257a07c1af0ecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not.

[4] Reward Protocol Whitepaper, available at https://rewardprotocol.com/wp-content/uploads/URP_Lightpaper-1.pdf. [Distributed app enabling retail geolocation.]

[5] Drew Robb, Building the global heatmap, Strava. November 1, 2017. https://medium.com/strava-engineering/the-global-heatmap-now-6x-hotter-23fc01d301de

[6] Andrew Liptak, Strava's fitness tracker heat map reveals the location of military bases, The Verge, Jan. 28, 2018. Available at: https://www.theverge.com/2018/1/28/16942626/strava-fitness-tracker-heat-map-military-base-internet-of-things-geolocation

individuals does not include advice to just opt out of all geolocation services. We simply cannot expect that people who are victims of violent crime never use a mapping app again. The better solutions right now are a lot of education about how device geolocation works, how app-level geolocation works, how a variety of platforms work with geolocation, and ensuring that any geolocation histories that are problematic are removed.

Overall, the biggest questions that come up repeatedly around geolocation include:

- How do consumers know when they are being tracked?
- What are the standard default settings for geolocation tracking?
- Is the burden always on consumers to opt out?
- Are opt outs always available?
- Is there a standardized opt-out for geolocation?
- What is being done with aggregate geolocation data?
- Is it possible to reidentify aggregate geolocation data that has been posted publicly?
- What are best practices around publishing aggregate geolocation data with a view to individuals' safety and privacy considerations?
- What are the best practices around geolocation and privacy/security settings?
- How many consumers understand the interaction between geolocation on device settings and app settings?

Although much work has already been done on geolocation, much more still can be done to both study consumer understandings of geolocation, and to set standards of what is acceptable disclosure around geolocation both on an individual and an aggregate level. If consumers have left on a default geolocation tracking setting, what does this mean for users who have subsequent privacy and safety challenges if the data is published? These are difficult issues, but these are the kinds of issues that need to be tackled. We see a number of positive advances the FTC can accomplish in this area.

We note here that in regards to geolocation, acceptable disclosure must be paired with the ability to turn off geolocation tracking. Some individuals have meaningful safety considerations. These individuals should be able to participate in geolocation when they need to, but not be forced to be tracked via geolocation when it is a safety concern for them or their children. And it should be exceedingly easy for consumers to switch geolocation off and on and be assured they are not leaving tracks. If a mistake has been made due to a lack of understanding or knowledge of default settings, consumer safety and protection needs to come first.

5. a. The efficacy of the Commission's use of its current remedial authority

[*Note: We are providing the same response for 5. a and 11. c.*]

-The Commission should bring more cases that rely on unfair practices

Because we believe that there is, in the larger view, little to be learned from deceptive practice cases, we ask the Commission to bring cases relying on the law banning unfair trade practices. What is needed in these cases is for the Commission to state positively and with more specificity what constitutes unfair conduct.

In the security area, there are plenty of statements of public policy, industry-adopted standards, and declarations of best practices so that the Commission should be able to base an unfairness case on clearly established and generally recognized principles. There is no need to for the Commission to create security standards out of whole cloth.

We observe that in the FTC's Ceridian case, the agency did include some language about unfairness. The complaint provided in paragraph 12:

> As set forth in Paragraph 8, respondent failed to employ reasonable and appropriate measures to prevent unauthorized access to personal information. Respondents' practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

The Commission's statement about unfairness in this case is too general to offer any real guidance. What is a *reasonable and appropriate measure*? The complaint does not say. The unfairness part of the complaint is really no more than one sentence. What must a company do to avoid a finding of unfairness? Is it unfair simply to suffer from a security breach?

We would like to see the Commission make a specific determination in a security case that it is unfair for a website processing personal information:

1) To not have a security policy;
2) to not conduct a risk analysis as part of its security policy;
3) to not employ sufficient encryption to protect personally identifiable information;
4) to not use password protection to limit access to data; and
5) to not require passwords to be changed routinely.

We offer this list as an example of the types of conclusions that the Commission could make in reaching a conclusion that a company's security practices are unfair. We realize that a complete list of security standards would be longer and more nuanced.

If the Commission were to use its existing authority to define in more detail what constitutes unfairness, it would go a long way to establish clearer standards for companies and produce better results for consumers. The specifics in the consent decrees in these cases do not yet accomplish these objectives. All that we typically know is that the company prosecuted did something to step over the line that separates acceptable

from unacceptable conduct. However, we have no idea where exactly the Commission draws that line.

Use of the Commission's unfairness jurisdiction has the ability to clarify the obligations of those who process personally identifiable information on websites and otherwise. There is little to be gained by pursuing deceptive trade practices one by one.

-Establish standards for security assessments

Related to the above comment about the need for the Commission to use its unfairness jurisdiction with more specificity, a tool that would help the agency accomplish this would be to create formal or baseline standards for security assessments. We do not have in mind that the agency establish a strict, inflexible template extending to hundreds of pages; rather, more of a mid-to-high level set of flexible and iterative guidelines giving some benchmarking ability for the agency as they conduct investigations and make decisions about practices.

Currently, the agency uses a reasonableness standard. Although this standard ultimately relies on current best practices, *reasonableness* is nebulous. A set of broad but clearer standards utilizing past FTC cases, industry best practices, NIST guidance, existing security audit knowledge, and other existing security tools could flesh out basics that define the contours of what constitutes *reasonable*.

We acknowledge the challenges in setting forth a benchmark of this sort, however, with opportunity for public input, and using existing best practices, it can be done. In creating a flexible standard that can grow and change with evolving practices, the agency could provide more meaningful guidance for industry and could potentially have more ability to bring cases based on unfairness.

-Establish standards for privacy assessments

We request that the Commission establish formal standards for privacy assessments. In our public comments that we submitted to the agency regarding the Uber matter,[7] we noted that it would be useful if the Commission held a public workshop on the subject of privacy assessments, with a goal of developing a staff report on the standards, content, and procedures for privacy assessments. We noted that there is also a need for clear rules governing the public disclosure of privacy assessments (or audits) mandated by the Commission.

We are concerned here that the consent decrees that the Commission puts forward to have a significant effect on the privacy practices of the companies that it investigates. A great deal of post-decree effectiveness rests on the effectiveness of benchmarking and proving

[7] Comments of the World Privacy Forum to the Federal Trade Commission regarding revised proposed consent decree, In the Matter of Uber Technologies Inc., File No. 152-3054 https://www.worldprivacyforum.org/wp-content/uploads/2018/05/WPF_Comments_re_Uber_revisedproposedconsent_052018fs.pdf

compliance. It will not be possible to benchmark privacy compliance if there are no specific benchmarks with with to accomplish this goal. Mandating 20 years of assessments that do not adhere to a meaningful standard or set of known benchmarks will do little to protect the interests of consumers. Given the gravity of privacy breaches such as what happened in the Facebook/Cambridge Analytica debacle, developing tools such as benchmarks and standards for assessing compliance is an important priority.

5. b. The identification of any additional tools or authorities the Commission may need to adequately deter unfair and deceptive conduct related to privacy and data security

The FTC needs the ability to engage in substantive rulemaking in the area of data privacy and security that is procedurally sound, timely, and in tune with the modern era. The FTC Operating Manual[8] states that the FTC rulemaking authorities range from narrow, such as the Wool Products Labeling Act, to more broad, such as Title I of Magnuson-Moss Warranty - FTC Improvements Act. The authorities are as follows:

1. The Clayton Act (1914), as amended by the Robinson-Patman Act (1936) (only for fixing quantity limits under §2(a))
2. Wool Products Labeling Act (1939)
3. Fur Products Labeling Act (1951)
4. Textile Fiber Products Identification Act (1965)
5. Fair Packaging and Labeling Act (1966)
6. Petroleum Marketing Practices Act (1978)
7. Title I of the Magnuson-Moss Warranty - Federal Trade Commission Improvements Act -- (1975) warranty provisions
8. Energy Policy and Conservation Act (1975)

While Magnuson-Moss does allow for FTC rulemaking, the act imposes substantive rulemaking limitations on the FTC. In particular, Magnuson-Moss carries with it significant procedural limitations and requirements that go far beyond rulemaking undertaken under the Administrative Procedure Act, or APA,[9] which directs agencies to undertake rulemaking in a fairly straightforward notice-and-comment process. There are ways the FTC can circumvent those rules, for example, Congress can request the FTC to conduct an APA-style rulemaking and specifically exempt it from Magnuson-Moss procedures. But the FTC is dependent on such exemptions to be free of the Magnuson-Moss procedures.

---

[8] Federal Trade Commission Operating Manual, Ch. 7, *Rulemaking*, available at https://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch07rulemaking.pdf.

[9] Administrative Procedure Act (APA), Pub. L. No. 79-404, 60 Stat. 237 (1946) (5 U.S.C. §§ 551–559, 701–706 (2012).

The FTC Operating Manual, Chapter 7.2.3.1 describes the limitations the Maguson-Moss Act imposed on FTC rulemaking authority:

> Effect of the Magnuson-Moss Warranty - FTC Improvements Act
>
> Section 202(a) of Magnuson-Moss provides that the Commission's §18 authority is its only authority to promulgate rules respecting unfair or deceptive acts or practices. Section 18 does not, however, affect the Commission's authority to prescribe rules (including interpretive rules) and general statements of policy with respect to unfair methods of competition in or affecting commerce. (See .4 below.)
>
> Moreover, the Magnuson-Moss amendments to the FTCA do not affect the validity of any rule that was promulgated under FTCA §6(g) prior to the date of enactment of those amendments. §202(c)(1) of Magnuson-Moss. In addition, the Magnuson-Moss enforcement procedures, i.e., civil penalty and consumer redress actions (FTCA §5(m)(1)(A) and 19), may be used with respect to violations of rules that were promulgated pursuant to the Commission's §6(g) rulemaking authority prior to the enactment of the Magnuson-Moss amendments.

The limitations created for the FTC under Magnuson-Moss were crafted in a much different world -- a world that existed prior to the modern Internet, prior to email, prior to social media platforms, prior to GDPR, and in short, prior to much of what the FTC is being required to oversee in the modern digital ecosystem. The Magnuson-Moss vision of how the FTC should operate is simply not a viable position for the FTC to be held to today, particularly in light of the privacy and security concerns attending the fast-moving data ecosystem, which have proven to be significant.

It is worth comparing the amount of time a Magnuson-Moss rulemaking can take, and the amount of time a more typical APA-style rulemaking can take. Under the Magnuson Moss rules, the FTC took 10 *years* to complete the rulemaking for the Disclosure Requirements and Prohibitions Concerning Franchising.[10] In 2009, acting on Congressional authority specifically exempting the FTC from having to use Magnuson-Moss rules, the FTC used APA rules to complete its Health Data Breach Rule. Notably, the FTC took 5 *months* to complete its 2009 Health Data Breach rule,[11] a rulemaking which WPF commented on.[12]

---

[10] Disclosure Requirements and Prohibitions Concerning Franchising ANPRM, February 28, 1997, 62 Fed. Reg. 9115. Disclosure Requirements and Prohibitions Concerning Franchising Rule, March 30, 2007, 72 Fed. Reg. 15,444.

[11] Health Breach Notification Rule, 74 Fed. Reg. 42,962 (Aug. 25, 2009). Health Breach Notification Rule NPRM, April 20, 2009, 74 Fed. Reg. 17914– 17925.

[12] World Privacy Forum, http://www.worldprivacyforum.org/wp-content/uploads/2009/08/WPF_FTCBreachcomments_06012009_fs.pdf

If the FTC is to act responsively to current data privacy and security problems, it needs the ability to act more quickly, as other agencies are able to do. It is well past time to lift the limitations of Magnuson-Moss from the FTC.

9. The consumer welfare implications associated with the use of algorithmic decision tools, artificial intelligence, and predictive analytics
Of particular interest to the Commission:
a. the welfare effects and privacy implications associated with the application of these technologies to consumer advertising and marketing campaigns;
b. the welfare implications associated with use of these technologies in the determination of a firm's pricing and output decisions; and
c. whether restrictions on the use of computer and machine learning and data analytics affect innovation or consumer rights and opportunities in existing or future markets, or in the development of new business models.

We are answering question 9 in relation to the use of algorithmic decision tools, AI, and predictive analytics and its subparts in one general response. Our response is based in large part on two substantive research studies we undertook. First, *The Scoring of America*[13] was published in 2014. Seven years in its research, *The Scoring of America* benchmarks specific applications, uses, techniques, and challenges with the uses of AI and predictive analytics. It was the first major privacy-focused analysis of AI that was published. Second, we are drawing from peer-reviewed original research on large-scale biometrics identity systems, researched and written by WPF executive director Pam Dixon, and published by Springer-Nature, subsequently published for Open Access with Harvard-based Journal of Technology Science.[14] *A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.* was the result of four years of research, including active fieldwork. Biometrics are an important subpart of AI and machine learning, and understanding the limitations and flaws in large-scale biometrics systems enables broader understandings of many aspects of AI and machine learning, as well as the where policy structures could improve outcomes.

We include these two publications into these comments by extension; as the research is quite extensive, we can only offer glancing high points here. Some of our points go into areas the agency's questions did not explore. We acknowledge the importance of the agency's questions, and also request that the agency consider the following issues as well.

---

[13] Pam Dixon and Bob Gellman, The Scoring of America: How secret scores threaten your privacy and your future, World Privacy Forum, April 2, 2014. Available at: https://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/

[14] Pam Dixon, A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S. Springer Nature, *Health Technology*. DOI 10.1007/s12553-017-0202-6. http://rdcu.be/tsWv. Open Access via Harvard-Based *Technology Science*: https://techscience.org/a/2017082901/.

-Framing the genuine tension points in AI and Machine Learning

Artificial Intelligence and machine learning techniques have matured considerably in the past decade, affording new insights into data across multiple disciplines. But for as much as it is discussed, there is not nearly adequate technical basis for discussion. This has led to a profound disconnect in the discussion.

- Different flavors of AI exist: **Convolution Neural Networks, Markov Models, Ensemble Methods, Deep Learning, Bayesian Belief Nets, Statistical Models.**

- These models have different levels of explainability: there are some **interpretable models, some models have the black box, modified deep learning techniques can learn explainable features.** It is crucial in policy discussions to distinguish between AI models and their differing levels of explainability.

- Much attention has been given to a variety of tension points in AI, for example, the lack of transparency of the "black box." However, additional tension points exist. And should be treated just as thoughtfully. Fairness, transparency, accountability, and good governance around uses of AI and multiple other aspects of AI are among key aspects to include in any principles and policies regarding AI.

- Two tension points in particular are often overlooked, that is, inputs risks, and risks regarding interpretation of results.

-Regarding inputs/data sets:

AI analysis is a data-intensive discipline, requiring abundant input factors ranging from raw data sets to algorithms, and in some cases, categorizations or scores based initially on raw data sets, a full accounting of the risks associated with input factors is important.

First, data sets must be available to use; second, data sets must be appropriately cleaned and prepared for use; and third**,** the data sets must be appropriately matched to the intended inferences or goals sought from the analysis. These are among the baseline considerations for data sets, understanding that many more considerations exist. Among these considerations includes potential issues relating to data sets that are derived directly from or about individuals or groups of individuals, or in some cases data sets that while not directly derived from or about individuals, can be used to create inferences about individuals or groups of individuals.

Consent and transparency of use are of particular importance for the use of data sets derived directly from or about individuals or groups of individuals. Ethical data use practices are a crucial aspect of governance, and should provide guidance as to which data sets create more potential risk for deleterious outcomes or use. Regarding algorithms or scores/categorizations used as input factors for AI analysis, a primary consideration

(beyond ethical data use) is that many of these types of input factors can be proprietary in nature. Given that some AI analysis utilizes numerous algorithms as input factors, proprietary algorithms could pose obstacles for AI use across industries or sectors over time, as well as pose substantial challenges to transparency, fairness, and interpretation.

-Regarding interpretation:

How to interpret the results of AI analysis needs specific governance, and should occur within an understandable, specific context and should be carefully constrained and defined. AI model results are only as predictive or as fair as the score model or models, the factors used in that model, and the training and fit of that model to the task or problem it was meant to solve for, among other factors. However, much interpretive nuance is easily lost when an AI model results in a simple numeric score.

A simple score can be deceptively complex to interpret; models can be over or under fit, creating potentially significant discrepancies in results. Over-fitting arises when an algorithm is trained to perform very well on an existing set of data, but has been tailored so well to that data set that it can behave erratically or incorrectly outside of the specific scenario it has trained for. When a predictive model assigns a value or a range to a person, for example, a risk score, the model used to create that value must be transparent, accurate, reliable, and kept up to date. The numeric range for interpreting the result (such as a score) should be well-quantified, and the results validated.

- Without these protections, even the best and most predictive model can be interpreted improperly, to potentially negative consequences.

- Currently, very little governance exists around the *interpretation* of AI results. It is an area particularly well-suited for further work.

-Innovation and restrictions on the use of algorithms/ML/ predictive analytics

India's building of a national digital biometric ID ecosystem is an important case study to understand in framing a balanced response to the question of balancing the drive for innovation and the need for protective restrictions on technology.

India went from adding its first enrollee in its Aadhaar biometric ID program in 2010, to boasting about more than 1 billion enrollees in 2016. In order to allow for innovation, growth, and modernization, regulations were eschewed in favor of technological advancement and modernization of the governmental, financial, health and other sectors. The Aadhaar digital identity ecosystem was intended to act as an identity key for the poor and to allow for unfettered delivery of subsidies. The vision was well-meaning, but the system suffered from multiple challenges that have caused the entire system to be brought into question.

One notable challenge the system experienced was significant mission creep, which caused a lack of trust in the system. Aadhaar went from being voluntary to being mandatory. Instead of just being used for delivery of subsidies, it became increasingly difficult to get paid, receive pensions, file taxes, bank, or get health services in India without an Aadhaar ID.

Second, the technical limitations of biometrics, which are well-studied and documented, created harms that the implementers did not anticipate. Across India, government reports faithfully noted extraordinary and mass "failures to authenticate." That is, individuals with Aadhaar IDs could not use their biometric IDs to authenticate themselves. The authentication problems stemmed from failures within the biometric system itself. At scale, statistically low rates of multi-factor or multi-modal biometrics systems can become millions of people who could not get food. In India, there have been reports of people dying because of failures to authenticate.[15]

The lesson for the US is that AI and ML systems need great care in planning, and if the systems rise to a level of public importance or widespread use or implementation, formal policy controls in the form of legislation must be in place well prior to installation. Unrestricted growth of a technology is not a panacea, and can lead to substantive harms as what were small errors turn into large harms at scale. And scale effects must be considered when answering any question balancing innovation and restriction of technology.

There are specific policy, procedural, and technological improvements that would have prevented many of the problems that now everyone can see in the Aadhaar system.

10.2. Whether the Commission can, and to what extent it should, take steps to promote harmonization between the FTC Act and similar statutes.

Promoting harmonization between the FTC Act and similar statutes is a helpful goal, as long as state-level "mini-FTC" statutes are allowed to remain intact without federal pre-emption.

Something that would be helpful in promoting harmonization would be for the FTC to establish privacy and security assessment/audit benchmarking standards, which could then also be used by other entities tasked with enforcing similar statutes. See WPF's response to 11.e and 5.c.

11. a. Whether the agency's investigative process can be improved without diminishing the ability of the Commission to identify and prosecute prohibited conduct

[15] Dhananjay Mahapatra, Don't let poor suffer due to lack of infrastructure for authentication of Aadhaar, Times of India, April 24, 2018. https://timesofindia.indiatimes.com/india/dont-let-poor-suffer-due-to-lack-of-aadhaar-tech-sc/articleshow/62842733.cms

We comment here only on the public-facing aspect of the agency's investigatory process.

- Update the procedures for communicating with the public about investigations

Traditionally, the FTC does not comment on ongoing investigations. This is fine. But WPF has submitted a number of complaints to the agency, and those complaints have heretofore gone into a vortex of silence, which in some cases, extends for years. One example is WPF's complaint filed against America Online (AOL) regarding its breach of users' search histories.[16] The Secretary acknowledged receipt of the complaint, but beyond that, WPF did not hear back on the results of an investigation, or even if there was one.

The FTC can do better than this. The model the CFPB uses, of at least opening a file and allowing consumers to be appraised of process and progress electronically, is a helpful one here. The FTC could allow groups filing complaints to have a contact point, and provide updates as to basic items such as if an investigation has been opened, if the investigation is closed, and so forth. The FTC could accomplish this without jeopardizing the integrity of investigations.

-Provide fact patterns to the public post-investigation

It would be helpful if the agency would provide ample fact patterns to the public after an investigation, particularly if the agency is requesting comment from the public. WPF has submitted a number of comments on proposed consent orders. However, it is rare for a robust fact pattern to accompany the request for comments unless there has been actual litigation. See for example, our difficulty commenting on the proposed consent order for Ceridian. [17]

While we understand why the agency cannot release all details of an investigation, we would like to see at least some portion of fact pattern released to the public so as to allow for informed decision making and analysis regarding any proposed consent agreement, or other decision the agency has taken.

11. c. The efficacy of the Commission's current use of its remedial authority

[*Note: We are providing the same response for 5. a and 11. c.*]

---

[16] World Privacy Forum Complaint to the FTC, In the Matter of America Online, August 16, 2008. Available at: http://www.worldprivacyforum.org/wp-content/uploads/2008/08/WPF_FTCcomplaint8162006fswp.pdf

[17] WPF comments regarding Ceridian, File No. 102 3160, p. 4. Available at: www.worldprivacyforum.org/wp-content/uploads/2011/05/WPF_CeridianFTCcomments_fs.pdf

-The Commission should bring more cases that rely on unfair practices

Because we believe that there is, in the larger view, little to be learned from deceptive practice cases, we ask the Commission to bring cases relying on the law banning unfair trade practices. What is needed in these cases is for the Commission to state positively and with more specificity what constitutes unfair conduct.

In the security area, there are plenty of statements of public policy, industry-adopted standards, and declarations of best practices so that the Commission should be able to base an unfairness case on clearly established and generally recognized principles. There is no need to for the Commission to create security standards out of whole cloth.

We observe that in the FTC's Ceridian case, the agency did include some language about unfairness. The complaint provided in paragraph 12:

> As set forth in Paragraph 8, respondent failed to employ reasonable and appropriate measures to prevent unauthorized access to personal information. Respondents' practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

The Commission's statement about unfairness in this case is too general to offer any real guidance. What is a *reasonable and appropriate measure*? The complaint does not say. The unfairness part of the complaint is really no more than one sentence. What must a company do to avoid a finding of unfairness? Is it unfair simply to suffer from a security breach?

We would like to see the Commission make a specific determination in a security case that it is unfair for a website processing personal information:

1) To not have a security policy;
2) to not conduct a risk analysis as part of its security policy;
3) to not employ sufficient encryption to protect personally identifiable information;
4) to not use password protection to limit access to data; and
5) to not require passwords to be changed routinely.

We offer this list as an example of the types of conclusions that the Commission could make in reaching a conclusion that a company's security practices are unfair. We realize that a complete list of security standards would be longer and more nuanced.

If the Commission were to use its existing authority to define in more detail what constitutes unfairness, it would go a long way to establish clearer standards for companies and produce better results for consumers. The specifics in the consent decrees in these cases do not yet accomplish these objectives. All that we typically know is that

the company prosecuted did something to step over the line that separates acceptable from unacceptable conduct. However, we have no idea where exactly the Commission draws that line.

Use of the Commission's unfairness jurisdiction has the ability to clarify the obligations of those who process personally identifiable information on websites and otherwise. There is little to be gained by pursuing deceptive trade practices one by one.

- Establish standards for security assessments

Related to the above comment about the need for the Commission to use its unfairness jurisdiction with more specificity, a tool that would help the agency accomplish this would be to create formal or baseline standards for security assessments. We do not have in mind that the agency establish a strict, inflexible template extending to hundreds of pages; rather, more of a mid-to-high level set of flexible and iterative guidelines giving some benchmarking ability for the agency as they conduct investigations and make decisions about practices.

Currently, the agency uses a reasonableness standard. Although this standard ultimately relies on current best practices, *reasonableness* is nebulous. A set of broad but clearer standards utilizing past FTC cases, industry best practices, NIST guidance, existing security audit knowledge, and other existing security tools could flesh out basics that define the contours of what constitutes *reasonable*.

We acknowledge the challenges in setting forth a benchmark of this sort, however, with opportunity for public input, and using existing best practices, it can be done. In creating a flexible standard that can grow and change with evolving practices, the agency could provide more meaningful guidance for industry and could potentially have more ability to bring cases based on unfairness.

- Establish standards for privacy assessments

We request that the Commission establish formal standards for privacy assessments. In our public comments that we submitted to the agency regarding the Uber matter,[18] we noted that it would be useful if the Commission held a public workshop on the subject of privacy assessments, with a goal of developing a staff report on the standards, content, and procedures for privacy assessments. We noted that there is also a need for clear rules governing the public disclosure of privacy assessments (or audits) mandated by the Commission.

We are concerned here that the consent decrees that the Commission puts forward to have a significant effect on the privacy practices of the companies that it investigates. A great

[18] Comments of the World Privacy Forum to the Federal Trade Commission regarding revised proposed consent decree, In the Matter of Uber Technologies Inc., File No. 152-3054 https://www.worldprivacyforum.org/wp-content/uploads/2018/05/WPF_Comments_re_Uber_revisedproposedconsent_052018fs.pdf

deal of post-decree effectiveness rests on the effectiveness of benchmarking and proving compliance. It will not be possible to benchmark privacy compliance if there are no specific benchmarks with with to accomplish this goal. Mandating 20 years of assessments that do not adhere to a meaningful standard or set of known benchmarks will do little to protect the interests of consumers. Given the gravity of privacy breaches such as what happened in the Facebook/Cambridge Analytica debacle, developing tools such as benchmarks and standards for assessing compliance is an important priority.

11. d. Willingness of affected parties to cooperate with the Commission in conducting post-investigation and enforcement retrospectives

In analyzing the effectiveness of FTC consent decrees *vis a vis* protecting consumer privacy and security over the long term, there are practical things that would assist the agency and the public in achieving a better outcome, including the following:

a. To require companies under consent orders to undergo a formal annual audit to particular benchmarking standards (ideally, a formal privacy and / or security standard);

b. to publish the audits publicly;

c. to require companies under consent orders to have a central and clear location online where consumers could complain about either their privacy or security practices, depending on the consent order; and

d. to require companies under consent orders to share consumer complaints with the agency and provide aggregate complaint reporting to the public annually, including number of complaints and type.

We recognize that some of the audit information may be sensitive, and thus would be potentially subject to redaction. This is fine. An overall approach that includes both benchmarking and transparency of results is the goal.

Currently, audits of companies under consent decrees can be requested via Freedom of Information Act (FOIA) requests made to the Commission. However, audits received through FOIA requests are likely be heavily redacted as allowable via FOIA Exemption 4, which covers trade secrets and commercial or financial information, among other information. This is a tricky area to find balance, and we recognize that.

Again, we believe that the public is better served by more transparency in this situation given the privacy and security interests of consumers.

Thank you for considering our comments. We are happy to provide more detail and information regarding the points we have made here, and would welcome the opportunity to discuss these important issues further.

Respectfully submitted,

Pam Dixon
Executive Director,
World Privacy Forum
www.worldprivacyforum.org
760-712-4281