Comments of the World Privacy Forum to the NTIA

Regarding

Developing the Administration's Approach to Consumer Privacy,
Docket No. 180821780-8780-01

Via email to: privacyrfc2018@ntia.doc.gov

Travis Hall, Telecommunications Policy Analyst
National Telecommunications and Information Administration
US Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, DC 20230

Dear Mr. Hall:

Thank you for the opportunity to comment on the NTIA's proposed approach to consumer privacy. The World Privacy Forum is a non-profit public interest research group that focuses on consumer data privacy issues, including those relating to emerging technologies, health, identity, data brokers, AI, and other topics. WPF is a non-political, non-partisan organization. WPF works exclusively on privacy, and is one of the few NGOs that focuses on creating objective research so as to produce fact-based consumer data privacy work. Our research, testimony, consumer education, and other materials are available on our webpage, www.worldprivacyforum.org.

We would be pleased to discuss our ideas about privacy legislation directly with the NTIA, and we welcome that opportunity. These comments discuss high-level structure of privacy thought and regulation, then discuss case studies that contextualize various principles presented in the NTIA Request for Comments.

It is our belief that we stand at a junction where significant technological shifts are creating an historic time of technological transition and a concomitant need to produce meaningful advancements in thought around data protection and privacy. In these comments, we sketch the outlines of what some of these changes might look like.

The need to move toward modern data governance

The privacy framework the NTIA is proposing is fine in many ways. It is, however, through no fault of its authors and contributors, old-fashioned. Approaches that worked for an era we are now passing out of are still being considered by the NTIA as primary solutions to privacy problems. But data is evolving, and privacy thought needs to similarly evolve. It is completely unnecessary to assign blame or shame. We are in a chaotic time of transition, and it is difficult to shift thinking into new models. But this is precisely what all of us must attempt.

The emerging world is one of rapid data transformation and data fusion. It requires an approach that will empower all stakeholders to participate in solutions and will provide an architecture for identifying, assessing, and mitigating privacy risk on an ongoing basis. This is modern governance, and correctly constructed, governance that will allow for a broadened approach to privacy and data that is collaborative, fair, and acknowledges the challenges of highly complex data environments. The challenges of the early Internet era are not the same challenges we face today. It therefore makes sense to adapt the frameworks we are using to solve new data-related problems.

Max Planck wrote about the evolution of physics theory in a 1909 essay,[1] explaining the challenges of the intellectual process of moving from Ptolemaic ideas to Copernican thought to Relativity theories. Physics thought has advanced further still in the years since Planck wrote his essay; were he to write his essay now, he would incorporate Quantum theories. The intellectual transitions, he wrote, brought forth "very great" resistance.[2] Today, in privacy thought, we need to adjust our thinking to adapt to the next phase of knowledge and data, and it would be to our advantage if this is accomplished sooner rather than later, despite how much resistance we may have.

The consequences of a misstep now regarding data governance frameworks will be consequential. Without an approach that correctly addresses new data paradigms, it will be difficult to compete with the technological advancements of the rest of the world. It will also be difficult to achieve sustainability in knowledge ecosystems — data is not the endless resource some perceive it to be, and people will not abide by abusive data systems over the long term. We can see hints and seedlings of some of the key emerging problems already, and we can similarly already see hints and seedlings of key solutions that can address emerging problems.

---

[1] Max Planck. Eight Lectures on Theoretical Physics, Delivered at Columbia University. "First Lecture. Introduction: Reversibility and Irreversibility. Dover: New York. 1998. "Certainly, the sacrifices demanded by every such revolution in the intuitive point of view are enormous; consequently, the resistance against such a change is very great. But the development of science is not to be permanently halted thereby; on the contrary, its strongest impetus is experienced through precisely those forces which attain success in the struggle against the old points of view, and to this extent such a struggle is constantly necessary and useful."

[2] Supra note 1.

The last 25 or so years of the Internet era was about the Internet as a General Purpose Technology.[3] This period of time saw the US and other jurisdictions moving at various rates from analog to digital systems. Within the US, the sectors digitized at different rates — for example, think of the rather rapid progression of music from CDs to Napster and MP3.com to iTunes and other digital music services that occurred from the 1990s onward,[4] as compared with the slower digitization of health sector data[5] during the same period of time. Evolution from single-point foci to more complex fusion systems is a hallmark of maturing systems. The era we are entering is hallmarked by a rich, highly complex fusion of data, and it mirrors this evolution toward system fusion.

The arriving era of data fusion is all about deep digital transformations, which extends far beyond mere digitization of data sets. The transformation goes beyond additive data layering and manipulation and moves into the creation of knowledge. To manage this transformation, we are not in need of only data protection, we are not just in need of only data governance, we are not only in need of privacy; we need systems that facilitate fair and just knowledge governance that are inclusive of data protection, inclusive of privacy, and are also fundamentally geared to address high complexity, rapidly evolving systems and their attendant risks and rewards on an ongoing basis.

The major trends such as AI, machine learning and its subsets like biometrics, all manner of large data sets and predictive analytics, the Internet of Things, mobile, cloud, and fully digital and dematerialized identity ecosystems are all emerging apace now. These technologies are fusing and converging to create something quite complex that we are just beginning to see the edges of. This is not the same world as the Internet as a General Purpose Technology. This "data fusion" is a world that is bringing new and novel tensions that legislative structures have not yet addressed.

We've seen versions of these kinds of significant technologically driven shifts throughout history. Most recently, early digitization brought an array of tensions which are now familiar to us. The laws enacted during the 90s and early 2000's reflect the growth pains of the time, for example, some of the first identity theft regulations and data breach regulations at the state level were passed as lawmakers learned about various risks of digitized data flowing in networks, including digitized identity data. In 2006, WPF coined the term "medical identity theft" and wrote the first report about the issue, recommending medical data breach notification as an important cure for the harms

---

[3] See Elhanan Helpman. General Purpose Technologies and Economic Growth. MIT Press, 2003. https://mitpress.mit.edu/books/general-purpose-technologies-and-economic-growth. See also: Rousseau & Jovanovic, General Purpose Technologies, Handbook of Economic Growth, Volume 1B. Edited by Philippe Aghion and Steven N. Durlauf , Elsevier 2005. http://www.nyu.edu/econ/user/jovanovi/JovRousseauGPT.pdf

[4] Stewart Wolpin, Flashback 1998: A compressed history of the digital music player. October 2018. https://www.soundandvision.com/content/flashback-1998-compressed-history-digital-music-player

[5] Micky Tripathi, EHR Revolution: Policy and legislation forces changing the EHR. *Journal of AHIMA* 83, no.10 (October 2012): 24-29. http://library.ahima.org/doc?oid=105689#.W-Y394qIafA

resulting from this crime.[6] Medical data breach notification was taken up as first a state-level policy, and eventually a national policy. In 2014, WPF wrote the first major report about consumer scoring and its risks, *The Scoring of America*.[7] This report focused on predictive analytics and the complex impacts the use of analytics has on individuals**.** Our conception of privacy had to broaden in the environment of scoring, and we began to discuss the meaningful marketplace impacts AI scores can have on peoples' lives, and what could be done to address the problems. It was through this work that it became clear that as we segue from a matured Internet era to an era of complex data fusion, some of the older ways of constructing privacy protections are not providing everything necessary to tackle real-world impacts.

Getting the right framework in place requires a different approach, because regulations need to address a nexus of transformational forces that are unruly and high-velocity.

Elinor Ostrom has articulated 8 principles regarding managing these types of frameworks. These principles are groundtruthed and based in actual practice. Ostrom wrote:

> Given the large variation in common-pool resources, their patterns of use, and their users, researchers agree that no single institutional design can be devised that will work in all of the many different common-pool resource situations. Researchers also agree, however, that we can discuss a set of general principles that increase performance of an institutional design (E. Ostrom 1990; Tucker 1999; Bardhan 1999).

The principles are as follows:

Rules are devised and managed by resource users.
Compliance with rules is easy to monitor.
Rules are enforceable.
Sanctions are graduated.
Adjudication is available at low cost.
Monitors and other officials are accountable to users.
Institutions to regulate a given common-pool resource may need to be devised at multiple levels.
Procedures exist for revising rules."[8]

---

[6] Pam Dixon, Medical Identity Theft: The information crime that can kill you. World Privacy Forum, May 3 2006. https://www.worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you/.

[7] Pam Dixon & Robert Gellman, The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future, April 2, 2014. https://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/.

[8] Nives Dolšak, Elinor Ostrom & Bonnie J. Mccay, The Commons in the New Millenium. MIT Press: 2003. See esp. Chapter 1, The Challenges of the Commons, New and Old Challenges to Governing Common Pool Resources.

Note that these principles are focused on governance, not content. Privacy content frameworks, like Fair Information Practices, work extremely well — but there has to be governance in place to contextualize and apply the policy ideas.

Some thoughts about knowledge governance frameworks and their role in managing complex data fusion systems:

1. Knowledge governance frameworks are a key component to incorporate in privacy and data protection work going forward. We conceive of knowledge governance as inclusive of data protection and privacy, and have the capacity to extend to additional core concepts, such as non-bias and fairness.
2. Governance needs to be iterative, and continually updated. "Living" governance is the key. NIST's Facial Recognition Vendor Tests are an excellent example of the application of this idea. In the past, NIST's tests were periodically conducted. Now, they are ongoing and iterative.[9]
3. Governance needs to identify and mitigate a complex and evolving array of risks. Risks should be assessed continually in a continual benchmarking of established rules against reality, and constant adjustment should be allowed based on actual, provable, repeatable feedback.
4. All stakeholders need to be involved in the conversation about shared resources, resources such as data and knowledge, and have appropriate power in the conversation and outcomes.Governance, to be effective for all stakeholders, needs to be collaborative.
5. Extreme data complexity, such as data fusion and knowledge creation, requires collaboration, not command and control approaches. In a collaborative framework, the structure can be set to allow for all stakeholders to achieve a win. Knowledge governance (which is inclusive of data protection and privacy) does not need to make a corporation or a user "lose" in order for another stakeholder to achieve a fair result.
6. To this end, corporations need to act responsibly as stewards of a shared data resource, in which end users often have a stake.
7. Individual users need to have agency to empower them to participate in data decision making, where appropriate. There needs to be a give and take with common pool resources. This can happen where treatment is fair, outcomes are unbiased and checked for risks.
8. There is a role for government as a stakeholder, particularly in enforcement.

It is positive that corporations take responsibility for a shared resource and manage it with care. It is also important to facilitate individuals' control over their personal data and enable them to participate in decision-making regarding the processing of their personal data throughout the data lifecycle.

---

[9] NIST FRVT 1:N 2018 Evaluation. https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-1n-2018-evaluation.

NTIA's Approach

We move now to the NTIA's published high-level goals of regulation:

1. Harmonize the regulatory landscape.
2. Legal clarity while maintaining the flexibility to innovate.
3. Comprehensive application.
4. Employ a risk and outcome-based approach.
5. Interoperability.
6. Incentivize privacy research.

Looking at the plain listing of ideas, we find agreement with many broad concepts.

- The regulatory landscape is fractured. But we see a core aspect of the problem as relating to laws representing older thought around data protection and privacy. Some laws, such as the Equal Credit Opportunity Act and the Fair Credit Reporting Act, remain vibrant and highly applicable despite changes in technology. Others, such as the Electronic Communications Privacy Act of 1986, are in need of updating to be more technology-neutral and adaptive to modern data flows.
- We see a possible role for state pre-emption in some rare cases, provided any law seeking to preempt state law provides a floor, not a ceiling, HIPAA being an excellent example of this. We respect and acknowledge the crucial role of innovation at the state level. Never forget that we can see our credit scores today because one state passed a law that required the credit bureaus to allow consumers to view their credit scores. State law has a major role to play in data protection and privacy. To lose this driver of innovation and risk mitigation would be to greatly reduce privacy innovation and would create deleterious consequences in the short and long term.
- A modern knowledge governance framework appropriately scoped and applied allows for legal clarity and flexibility and consumer protection. Command and control legislation that locks parties into a static regulation is not preferable, neither is regulation that creates winners and losers.
- Risk and output analysis is important, but it is not absolutely everything. The way we articulate this broadly is that technology use must do no harm, and must create a public good.
- Interoperability today, as the NTIA discusses it, is going to be tied to the standard of the General Data Protection Regulation of Europe. Europe is a significant economic jurisdiction, and has created standards that will be in play for decades. This is a reality that the NTIA will have to address rather than avoid.
- We fully agree that privacy research needs to be incentivized. Broad and diverse funding would certainly be helpful to facilitate this. Research on risk analysis innovation will be important.

However, a significant omission in the goals of regulation is the omission of governance framework guidance. Principle 4 is insufficient to provide practical guidance on how to device rules in diverse and complex data systems. The Ostrom principles could be adapted and would be an important addition.

NTIA Principles: Case Studies (Data brokers, AI and machine learning, FTC enforcement, national-level Biometric implementations.)

The NTIA has set forth the following specific principles:

- Organizations should be transparent about how they collect, use, share, and store users' personal information.
- Users should be able to exercise control over the personal information they provide to organizations.
- The collection, use, storage and sharing of personal data should be reasonably minimized in a manner proportional to the scope of privacy risks.
- Organizations should employ security safeguards to protect the data that they collect, store, use, or share.
- Users should be able to reasonably access and correct personal data they have provided.
- Organizations should take steps to manage the risk of disclosure or harmful uses of personal data.
- Organizations should be accountable for the use of personal data that has been collected, maintained or used by its systems.

Some aspects of these principles are helpful. However, taken as a whole, overall this approach does not provide for key aspects of modern data governance, as we have discussed. As a result, we see meaningful gaps in protections, and overall, there is still a need to provide a wholistic solution that addresses the full range of modern privacy problems. In order to illustrate this, we would like to apply several case studies: secondary data uses by data brokers, consumer scoring using machine learning and AI techniques, biometrics implementation on a national scale, and FTC enforcement.

Case Study: Data Brokers

Privacy legislation in the U.S. has a long and storied history. However in all of the rich legacy of privacy law there exists a gap that is still unresolved: there are not controls over most secondary uses of data and tertiary sales or uses of consumer data. Nowhere has this deficit been more problematic than in the data broker industry. The World Privacy Forum has spent years researching and documenting data broker practices.

Our research has found:

- Data brokers sell, trade, and share highly sensitive and identifiable information about consumers – usually without any knowledge on the part of consumers about these activities.WPF has meaningfully and repeatedly documented that data brokers sell information about consumers who have bought a particular item, take certain medications,

read certain books, or engage in certain activities.[10] Thousands of data broker lists exist, with millions of consumers identified in the lists by name.[11]

- The data broker industry has evolved to also focus on detailed consumer data analysis that results in predictive profiles of consumers, often with a score attached. WPF calls this "consumer scoring," and we documented these practices extensively in our report, *The Scoring of America*.
- Consumer scoring covers everything from consumer loyalty to employability to personality scores to medical risk scores, and more. These analytical scores become a kind of shorthand to describe consumers and can influence meaningful marketplace opportunities in consumers' lives. Again, without consumers' knowledge or control.[12]
- Data brokers, data compilers, large technology platforms, and entities with large data stores do not have absolute control of tertiary uses of data, including malicious uses. Consumers in particular do not have enough controls over their data. Real consumer harms can result from secondary and tertiary uses, and the harms can continue forward for years in some cases. When consumer data escapes into third party hands, there are almost no existing controls for fully recapturing the escaped data or fully understanding everywhere the data might have gone. This is illustrated by the Facebook Cambridge Analytica scandal, by the Equifax data breach, and many others.

Solving the problem of applying meaningful controls of secondary and tertiary sales and uses of consumer data must be at the core of what gets resolved in any federal privacy legislation. If federal privacy legislation does not address this set of core issues, then the secondary uses gap will continue unabated, and no real privacy can be had as long as this gap exists. This gap can be narrowed by meaningful work to provide:

- Consumer controls of certain data flows and data uses, including long-term controls,
- Creating transparency, choice, and meaningful rights around consumer scoring,
- Creating technological, procedural, and policy controls over secondary and tertiary data uses. This can range from data tracking techniques to standards for de-identification to technological measures that audit data for inappropriate/appropriate uses over its lifetime.

No one expects perfect solutions. But if proposed solutions do not directly and clearly address the lynchpin of the consumer privacy data challenges related to data brokers, then we will not accomplish what we need to.

---

[10] See World Privacy Forum, Congressional Testimony Page: https://www.worldprivacyforum.org/category/congressional-testimony/.

[11] See Nextmark List Finder, https://lists.nextmark.com/market. The List Finder is a search engine for data broker lists.

[12] For a recent article about consumer lifetime value scores, see On hold for 45 minutes? It might be your secret consumer score. Khadeeja Safdar, Wall Street Journal, Nov. 1, 2018. https://www.wsj.com/articles/on-hold-for-45-minutes-it-might-be-your-secret-customer-score-1541084656.

Taking some of the NTIA principles and applying them to data broker activities, let us look at the idea, for example, the NTIA articulates of users having control over the data *they* provide to entities. Does this principle work to solve data broker issues?

First, think of the case when users, as they use debit or credit cards to make purchases, are in fact providing their card data to retailers. They are doing so to make a purchase. Nevertheless, we know that retailers can and have shared and sold this data to data brokers as a secondary use of the data.[13] How can a user exercise meaningful control over this and similar secondary use situations that occur downstream without their knowledge? It is not sufficient to say to consumers that they should simply pay with cash and never shop online. It is unlikely that federal legislation will tell business to stop selling data. The NTIA principle here does not address data broker risks and harms.

Second, in regards to having control only over data input by the consumer, it is not only about what data a user provides specifically to an organization that is meaningful. Also meaningful is the knowledge that can be created utilizing that original data. This new knowledge is more than the sum of its parts. Going back to the use of retail purchases as a data set, we documented the issue of consumer prominence scores, or consumer lifetime value scores in *The Scoring of America*. These scores, which are in part based on consumers' retail purchase data, can create risk and have a real-life impact on how a consumer is treated in multiple service and retail contexts, among other situations.

Conversely, user data that is compiled and transformed can be used to create meaningful new data sets that provide data groundwork for medical, societal and other advances, and in so doing, create public benefit.[14] How does user control work in these circumstances? The best parties to determine the answer to this and other questions are the stakeholders involved. Smaller ecosystems can be managed with more specificity and stakeholders can arrive at solutions that are iterative and provide all parties with the ability to achieve benefits and goals.[15] But there has to be a governance mechanism that facilitates achieving these outcomes.

Case Study: 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. 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 so-called "black box" which can be impenetrable, for

---

[13] See *Scoring of America*.

[14] See for example, Centers for Disease Control data sets: https://www.cdc.gov/nceh/data.htm.

[15] See, generally, the work of Elinor Ostrem. The Commons in the New Millenium: Challenges and adaptation. MIT Press: 2003. See esp. Chapter 1, The Challenges of the Commons, New and Old Challenges to Governing Common Pool Resources.

some models, 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 risks:

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. This would likely fall under risk mitigation in the NTIA model. However, it is not clear that the risk to end users is possible to fully address in the NTIA model as currently articulated.

Part of the reason for the is the NTIA model does not fully address consent and transparency of use — it is simply not possible for some models to be totally transparent. What direction is available for these situations? Transparency is 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. The NTIA model deals with proprietary issues by simply stating that in all situations, only the data the user provides is protected. This sets up a win-lose situation.

Regarding interpretation of AI outputs:

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.
- Governance models can be used to address the numerous contextual issues that arise.

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

The NTIA principle that articulates that consumers could control information they have provided is intended to help companies work with data and give consumers some degree of control. The approach attempts to seek a balance, but it does so without using continual feedback from consumers about risk and impact. It does so without setting parameters with input from all stakeholders to begin with.

Moreover, the principle as written does not address data transformation. By leaving data transformation out of the principle, this has the unfortunate consequence of creating disparities of power among stakeholders, eventually leading to consumer anger and lack of trust, and all manner of data abuse that consumers are growing to deeply dislike. Companies that want to act ethically and responsibly are already moving past this approach in favor of more responsible and collaborative approaches that are friendlier to end users.

An additional question arises regarding how this principle works with data portability. Data portability is an aspect of user control of data. Data portability will apply quite differently based on the context of the data. A governance framework will facilitate input from all stakeholders in specific contexts and will allow all participants to understand and work out the specifics. Otherwise, the principle doesn’t adapt well to varying contexts.

Case Study: Role of the FTC in Enforcement of Privacy

There is an important role for government stakeholders in modern governance frameworks. In the US, the FTC is the most suitable agency to be utilized for enforcement of data protection and knowledge governance. In order to do so, the FTC needs more staff, more breadth of purpose, and 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. It is important to have a framework for defining stakeholders and their roles.

The FTC Operating Manual[16] 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 FTC's 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
8. Improvements Act -- (1975) warranty provisions
9. 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,[17] 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.

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

---

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

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

> 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.[18] 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.[19] Notably, the FTC took 5 months to complete its 2009 Health Data Breach rule,11 a rulemaking which WPF commented on.[20]

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.

---

[18] 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.

[19] 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.
If

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

Case Study: Large-scale biometric implementations and data governance

This case study comes to us from India, which has provided the world's most significant case study on the implementation of nation-wide biometric systems. Why is this relevant? Because government stakeholders have important roles in any data and privacy framework. Also, in the US, government stakeholders are in the process of implementing biometric systems in airports. How this is accomplished matters a great deal. India's building of a national digital biometric ID ecosystem, which is called the Aadhaar identity 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 when the government is a major stakeholder. [21]

India went from adding its first enrollee in its Aadhaar biometric ID program in 2010, to boasting more than 1 billion enrollees in 2016. In order to allow for innovation, growth, and modernization, privacy and data protection 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, frictionless 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, and ultimately, the system has now been sharply curtailed.

One notable challenge the system experienced was significant mission creep, which caused a lack of user trust in the system over time. 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. As the Aadhaar become used more widely, Aadhaar also went from being a voluntary system to a mandatory system.

Another challenge existed in the technical limitations of biometrics, which are well-studied and documented. These technical limitations 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

[21] 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/.

people who could not get food. In India, there were reports of people dying because of failures to authenticate.[22]

One lesson for the US is that technology 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. Also key is talking with the user stakeholders and giving them appropriate power. User stakeholders being the public. 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.

In regards to the NTIA principles, the principles do not address some of the extremely complex challenges the large and complex systems in India created. Again, there are specific policy, procedural, and technological improvements that would have prevented many of the problems that now most everyone can see in the Aadhaar system. The NTIA guidance does not address roles of stakeholders, and responsibilities and duties of stakeholders. This will be an important aspect of any guidance. It would serve the US well as it begins to install biometric technologies in airports.

Conclusion

Most privacy experts can agree that there are gaps in privacy protections today that matter in peoples' lives. What people disagree on is how to close the gaps. Whether individuals disagree about installing a pure FIPs program or a modification thereof, whether individuals disagree about pre-emption and patchworks and many other areas of disagreement, the one thing we can potentially find some agreement on is that moving forward, we will need to find a way to work with data resources in a way that is cooperative, that allows for win-win solutions that appropriately empower all stakeholders, that address and mitigate risks on an ongoing basis, and that at the end of the day, intentionally avoid causing harm and create a public good.

Thank you for considering our comments.

Respectfully submitted,

S/

Pam Dixon
Executive Director,
World Privacy Forum

---

[22] 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