



WORLD **PRIVACY** FORUM

3 Monroe Parkway
Suite P #148
Lake Oswego, OR 97035

**Comments of the World Privacy Forum
to the Federal Trade Commission
Regarding Hearings on Competition and Consumer Protection in the 21st Century;
Docket ID: FTC-2018-0098, Consumer Privacy and
Docket ID FTC-2018-0101, Algorithms, Artificial Intelligence, and Predictive Analytics**

Via [regulations.gov](https://www.regulations.gov) and via email to CCPhearings@ftc.gov

Federal Trade Commission
Office of the Secretary,
Room H-113 (Annex X)
600 Pennsylvania Avenue, NW
Washington, DC 20580

December 28, 2018

Thank you for the opportunity to comment on consumer privacy, consumer privacy legal frameworks, potential federal regulation, and critically important related issues such as the role of the FTC in oversight of data ecosystems, ongoing challenges with data brokers, and AI governance. These comments relate to privacy and legal frameworks, as well as AI topics. We are filing these comments simultaneously under two dockets: **FTC-2018-0098** and **FTC-2018-0101**.

The World Privacy Forum (WPF) is a non-profit public interest research group that focuses on consumer data privacy issues, including those relating to emerging technologies, identity, data brokers, AI, health, and other topics. WPF is a non-political, non-partisan organization. WPF works exclusively on privacy and data protection, and is one of the only NGOs that focuses on 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.

These comments outline our thinking on privacy, privacy governance, and key priorities for federal privacy legislation.

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 this might look like and where advances might be most possible, practical, and helpful.

Specifically, these comments include a discussion of the following points:

I. Privacy Principles and Data Governance

II. The Role of the FTC in Modern Governance Frameworks

III. Case Studies:

Data brokers

AI and machine learning,

Biometrics

Throughout these comments, several key ideas resurface, one of which is the importance of mutual trust among privacy stakeholders. Any federal privacy legislation needs to solve for multiple problems. In a deep analysis, a breakdown of mutual trust and its consequences is among the roots of multiple problems we face in privacy. These comments articulate approaches that address how to advance privacy thought, and begin to solve the problems of trust breakdown in privacy, which appears to be a problem that is getting worse.

In addition to these comments, we are submitting as a separate comment our Scoring of America report, which benchmarks and articulates many findings and recommendation around data, data brokers, and predictive analytics.¹

I. Privacy Principles and Data Governance

A. Introduction

Data is evolving, and privacy approaches need to similarly evolve. 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 in order to genuinely and effectively address the very real privacy and knowledge governance problems we face.

¹ Because the *Scoring of America* sets a series of benchmarks for predictive analytics, and the data is still valid, we attach the *Scoring* report in full as a formal addition to our comments. We will file it separately for ease of access.

The emerging data world is one of rapid data transformation and data fusion. It requires an approach based on sturdy privacy principles (such as the existing Fair Information Practices, or FIPs model)² combined with, or layered with, knowledge governance principles (such as those articulated by Nobel Laureate Elinor Ostrom, discussed more below.) Joining FIPs (or other baseline privacy principles) with governance principles inclusive of due process will allow for mutuality in data and privacy solutions and will provide an architecture for identifying, assessing, and mitigating privacy risk on an ongoing basis.

This kind of framework consisting of FIPs plus modern governance, correctly constructed, creates a system of knowledge 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. It is not feasible to continue forward attempting to adapt privacy frameworks primarily to the individual control model — the data ecosystems have become too complex for relying on this approach.

It is important to pause here and articulate that the “FIPs plus governance” structure referred to here may mention the term risk, but what we are articulating is not the same as what is today commonly referred to as a “risk based approach,” which is a much more narrow concept. The idea of principles plus specific governance principles is much more than that, and is effective for complex systems utilizing shared resources (data, information, knowledge) and has already been extensively field-tested in other disciplines.

Without an approach that correctly addresses new and complex 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. Data as a shared resource requires all of the stakeholders to have mutual trust; otherwise, in the absence of trust, to function, data ecosystems often resort to hierarchical, non-transparent, inflexible and less than democratic approaches to data use and control. Ultimately, command-and-control use of data is not a

² Robert Gellman. *Fair Information Practices: A Basic History*. V. 2.18, April 10, 2017, <https://bobgellman.com/rg-docs/rg-FIPshistory.pdf>. See also: HEW Report: Records, Computers and the Rights of Citizens Report of the Secretary's Advisory Committee on Automated Personal Data Systems July, 1973. Available at: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>

sustainable activity. History is littered with examples of large and even national-level data ecosystems which failed after end-user stakeholders lost trust in those systems and their controllers.³ The growing lack of trust⁴ between parties (consumers, companies, other stakeholders) is the core basis of a detrimental social trap, as described by Bo Rothstein and others.⁵ In the wake of multiple large data breaches, and in the ongoing response to data scandals such as Cambridge Analytica,⁶ the importance of trust should be understood to be of central importance. WPF has long predicted that as people become more aware of data brokers,⁷ and in particular, of expansive uses of individuals' retail

³ The now disbanded UK National ID Card System is an exemplar of a system that experienced failure at a national level. The system, approximately 8 years in the planning, was launched and partially implemented, but was not trusted due to highly intrusive, non-voluntary measures many of those who were to be subject to the cards objected to. The system was disbanded just after its launch, at significant expense. For background, see: Alan Travis. *ID cards scheme to be scrapped within 100 days*. The Guardian, 27 May, 2010. Available at: <https://www.theguardian.com/politics/2010/may/27/theresa-may-scrapping-id-cards>. The £ 4.5 billion UK system, which was envisioned to encompass an ID register, biometric passports, and a mandatory ID, was scrapped after 15,000 ID cards were already issued. Legislation was passed abolishing the system in 2010; The Identity Documents Act 2010 repealed the Identity Cards Act 2006. See Identity Documents Act 2010. Parliament, UK. Available at: <https://services.parliament.uk/bills/2010-11/identitydocuments.html>

⁴ The US Census Bureau collected significant national consumer research regarding privacy and trust in July 2015. The results were given to the NTIA and form the basis of an extensive national survey and analyses published in 2016. NTIA, based on the survey results, found that a lack of consumer trust was negatively impacting economic activity. The NTIA noted: "Perhaps the most direct threat to maintaining consumer trust is negative personal experience. Nineteen percent of Internet-using households—representing nearly 19 million households—reported that they had been affected by an online security breach, identity theft, or similar malicious activity during the 12 months prior to the July 2015 survey." See: NTIA, *Lack of trust in Internet privacy and security may deter economic and other online activities*. May 13, 2016. Available at: <https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>.

⁵ A social trap is a situation where cooperation between individuals, groups, organizations, multi-stakeholders, or societies has become impossible due to mutual lack of trust. See in particular Bo Rothstein. *The Quality of Government: Corruption, Social Trust, and Inequality in International Perspective*. University of Chicago Press, 2011. See Ch. 7 and discussion of social trust and the consequences of its loss: "...Since agents in a group that have lost trust in one another cannot easily mimic or fabricate the level of trust needed to ensure collaboration even if they all know they would benefit if they could (Ostrom 1998; Rothstein 2005)." See also Bo Rothstein. *Social Traps and the Problem of Trust*. University of Cambridge Press, 2005. <https://www.cambridge.org/core/books/social-traps-and-the-problem-of-trust/02225C0BB48764F18F287FD6569EEF2E#fndtn-information> See also: Bo Rothstein, *The Chinese Paradox of High Growth and Low Quality of Government: The Cadre Organization Meets Max Weber*. Governance: An International Journal of Policy, Administration, and Institutions, Vol. 28, No. 4, October 2015 (pp. 533–548). doi:10.1111/gove.12128

⁶ Multiple authors. *The Cambridge Analytica Files: A Year-Long Investigation into Facebook, data, and Influencing Elections in the Digital Age*. The Guardian. Available at: <https://www.theguardian.com/news/series/cambridge-analytica-files>

⁷ The state of Vermont, the first to pass data broker legislation, defines data brokers in its 2018 statute as: "a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship." See: H.764, An act relating to data brokers and consumer protection. <https://legislature.vermont.gov/bill/status/2018/H.764>

and financial transactional histories, that this will create additional serious trust issues, which in turn can lead to a lack of cooperation, to everyone's detriment.

In these comments, we discuss our current data ecosystem, and how we might go about regaining trust and moving toward a system of knowledge governance that reduces and prevents social traps.

B. The Evolution of Complex Data Ecosystems: From the Internet as a General Purpose Technology to Data Fusion

The last 25 or so years of the Internet era was about the Internet as a General Purpose Technology.⁸ 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,⁹ as compared with the slower digitization of health sector data¹⁰ 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.

⁸ See Elhanan Helpman. [General Purpose Technologies and Economic Growth](https://mitpress.mit.edu/books/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>

⁹ 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>

¹⁰ 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>

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 resulting from this crime.¹¹ Medical data breach notification was taken up as first a state-level policy in California, and eventually became a national policy.

In 2014, WPF wrote the first major report about consumer scoring and its risks, *The Scoring of America*.¹² 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 complex environment of scoring, and we began to discuss the meaningful marketplace impacts AI-generated 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.

In the ensuing years, the issues we raised in *The Scoring of America* have continued to percolate apace; for example, recent headlines regarding the unfairness and ugliness of Consumer Lifetime Value scores, something we discussed and included in the Scoring report, are being met with surprise and unhappiness by consumers.¹³ The challenges associated with complex data environments have not been solved by the current frameworks that are in place.

Getting the right framework in place now requires an expanded approach, because regulations need to address a nexus of transformational forces that are unruly and high-velocity. And regulations need also need to address the trust and other complex issues that have complicated solving privacy challenges.

¹¹ 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/>.

¹² 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/>.

¹³ Khadeeja Safdar. *On Hold for 45 Minutes? It Might be your Secret Customer Score*. Wall Street Journal, Nov. 1, 2018. Available at: <https://www.wsj.com/articles/on-hold-for-45-minutes-it-might-be-your-secret-customer-score-1541084656>

C. Data as a Shared Resource: Ostrom's 8 Principles for Managing Common-Pool Resources

Nobel Laureate Elinor Ostrom spent her entire career observing governance of complex ecosystems. Over years, she observed and distilled the most effective ways of managing complex ecosystems where stakeholders share resources ("common pool" resources). Ostrom set forth 8 principles for governance of complex systems using shared resources. The Ostrom 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 Ostrom general principles are as follows:

1. Rules are devised and managed by resource users.
2. Compliance with rules is easy to monitor.
3. Rules are enforceable.
4. Sanctions are graduated.
5. Adjudication is available at low cost.
6. Monitors and other officials are accountable to users.
7. Institutions to regulate a given common-pool resource may need to be devised at multiple levels.
8. Procedures exist for revising rules."¹⁴

These principles are focused on governance, not content of principles or laws specific to the ecosystem.

The Ostrom governance principles were originally derived from observations in complex environmental ecosystems. They can also be applied in complex data ecosystems where privacy frameworks such as FIPs provide baseline principles to apply and implement. Just as privacy impact assessments originated from environmental impact assessments,¹⁵ the Ostrom principles that have worked to govern complex environmental and other ecosystems can work to create desired privacy outcomes in complex data and knowledge ecosystems.

¹⁴ 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*.

¹⁵Bamberger, Kenneth A. and Mulligan, Deirdre K., *PIA Requirements and Privacy Decision-Making in US Government Agencies*. July 22, 2012. D. Wright, P. DeHert (eds.), *Privacy Impact Assessment (2012)*; UC Berkeley Public Law Research Paper No. 2222322. Available at: <https://ssrn.com/abstract=2222322> **See also:** Roger Clarke, *A History of Privacy Impact Assessments*. Available at: <http://www.rogerclarke.com/DV/PIAHist.html> Roger Clarke. **See also:** Roger Clarke, *Privacy Impact Assessment: Its origins and development*. *Computer Law & Security Review*, Vol. 25, Issue 2. 2009. <https://doi.org/10.1016/j.clsr.2009.02.002>

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.¹⁶ Privacy governance frameworks need to be similarly responsive.
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 the opportunity 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 and not dominated by certain participants. For this to happen, due process rules for creating multi-stakeholder rules will need to be employed, formal rules such as those in the ANSI *Essential Requirements*¹⁷ will be crucially important.
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. The decision making should occur at the beginning and throughout the process, beginning with

¹⁶ NIST FRVT 1:N 2018 Evaluation. <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-1n-2018-evaluation>.

¹⁷ American National Standards Institute. *ANSI Essential Requirements: Due process requirements for American National Standards*. Edition: Jan. 2018. <https://share.ansi.org/Shared%20Documents/Standards%20Activities/American%20National%20Standards/Procedures%2C%20Guides%2C%20and%20Forms/ANSI-Essential-Requirements-2018.pdf>. The ANSI standards require openness, lack of dominance, balance, coordination and harmonization, notification of standards development, consideration of views and objections, consensus vote, appeals, and written procedures. There are also benchmarking procedures and compliance procedures with the rules.

setting rules and moving through to the end points. However, it is no longer feasible to base privacy frameworks on the ideas of solely individual control.

8. There is a role for government as a stakeholder, particularly in enforcement. (See discussion of the FTC's role in these comments.)
9. It is not possible to overstate the need to avoid and prevent social traps, such as the development or worsening of a lack of trust between stakeholders. The lack of trust or a basis upon which to build trust is a very significant problem that needs to be addressed. Governance will help, but only if it is based on mutuality, not command and control structures where end users do not have a seat at the table and where certain actors are allowed dominance.

It is positive that corporations take responsibility for a shared resource and manage it with care. However non-dominance is also important. Rules that facilitate all stakeholders' - including individuals' — ability to participate in decision-making regarding the processing of their personal data throughout the data lifecycle. Not through a series of ever-more-complex check boxes and consents, but through decision-making about the outcomes.

No system for privacy will be perfect. But combining privacy principles such as FIPs *with* knowledge governance as articulated by Elinor Ostrom gets us much further down the road than ecosystem governance designs that exhibit over-reliance on end-stage checkbox consent mechanisms, among other individual-level control mechanisms that ultimately cannot solve emerging data protection issues in a volatile, complex data environment.

II. The Role of the FTC in Modern Governance Frameworks

One of the core aspects of governance as theorized and ground-truthed by Ostrom is that when shared (data) resources are determined to create (privacy) risk, then a principles / code of conduct process would need to begin to allow all stakeholders to participate in determining the appropriate uses of that resource. The rules for how to conduct this kind of specific privacy standards creation process could be articulated through rulemaking, which we propose the FTC would undertake.

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 independence, 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.

In the past, the creation of specific standards of privacy conduct for sectors, slices of sectors, and certain technologies has been an area of considerable difficulty. WPF has written about and documented the difficulty in our report about the challenges and failures of privacy self-regulation.¹⁸

¹⁸ Robert Gellman and Pam Dixon. *Many Failures: A brief history of privacy self-regulation*. World Privacy Forum, 2011. Available at: <https://www.worldprivacyforum.org/2011/10/report-many-failures-introduction-and-summary/>

What we envision here is not the privacy self-regulation of old; it is a different system that has appropriate checks and balances and is based on mutuality, as defined first in the HEW report and then expanded upon by Ostrom's work and made practical by, for example, the *ANSI Essential Requirements*.¹⁹ Creating a replicable, cooperative way to understand and create the conditions for social trust also plays a role in solving today's privacy challenges.

A. The FTC and Governance Standards Creation Process

If a principles framework such as FIPs were in place, and were connected to a governance framework based on mutuality, such as Ostrom's, the FTC would have an important role in ensuring that the governance aspect of the system was appropriate, fair, and mutual. After those conditions are in place, then the conditions of trust and the capacity for creating a dialogue can be fostered and built.²⁰

Here is how a FIPS + Governance system could work at a practical level:

FTC Authority to oversee privacy standard making, and aspects of standards-setting

- The FTC would have the authority to oversee standards or principles set, or codes of conduct.
- The rules for the creation of such standards or principles or codes of conduct would be determined by statute, or by rulemaking, and the creation of the principles would need to abide by certain specific rules.
- If the rules were not followed, the FTC could step in and enforce against this.
- For example, if a company said they were writing principles to create great privacy guidance around Facial Recognition technologies, that company would need to abide by standardized rules for **how to create those principles**.

Standards Setting Process, and Rules for Due Process

- A process of ongoing analysis that includes multiple stakeholders would need to be active to identify areas of increased privacy risk that require additional rules to govern the data resources and outcomes.
- After a principles process was triggered, in the Ostrom model of governance, there would be a standardized procedure for creating the actual principles. For example, there would be an

¹⁹ *Supra* note 17.

²⁰ See Bo Rothstein. *Social Traps and the Problem of Trust*. Cambridge University Press, 2005. See in particular Chapters 8 and 9.

opportunity for comment, there would be transparency, all stakeholders would be engaged, and so forth.

- The World Trade Organization (WTO), *Agreement on Technical Barriers to Trade*²¹ is a core document that outlines how standards may be set by independent parties in a fair and appropriate manner that does not create transactional or, for applicability to data ecosystems and privacy risks. The American National Standards Institute (ANSI) produces a detailed standard for standards setting, which is the *ANSI Essential Requirements: Due process requirements for American National Standards*.²² The ANSI standards require openness, lack of dominance, balance, coordination and harmonization, notification of standards development, consideration of views and objections, consensus vote, appeals, and written procedures. There are also benchmarking procedures and compliance procedures with the rules.

With rules such as WTO's *Agreement on Technical Barriers to Trade* and the *ANSI Essential Requirements*, it would mean that when any group of stakeholders want to create standards for a particular setting, there would be a known procedure for doing so, one with checks and balances to avoid trust problems, power imbalances, and poor quality. A company or a group could not just sit down and self-determine standards without engaging all stakeholders and following the rules.

Standards Oversight and Enforcement:

The FTC could be given the authority to declare as an unfair and deceptive act and practice any set of principles that had not been created according to the established rules, and had not been inclusive of all stakeholders. This would create enforcement for principles created while at the same time not requiring the FTC to directly participate in each process.

For the above to happen, federal privacy legislation would need to contemplate and include a process for governance and principles oversight, and the FTC would need to be given more independence and would need broad rulemaking authority.

A note here: earlier we mentioned the problems of “social traps.”²³ When lack of trust between data stakeholders exists, this is a consequential problem. Lack of trust between stakeholders prevents the movement from hierarchical “command and control” legislative and regulatory approaches to

²¹ World Trade Organization, *Agreement on Technical Barriers to Trade*. Available at: https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm

²² American National Standards Institute. *ANSI Essential Requirements: Due process requirements for American National Standards*. Edition: Jan. 2018. <https://share.ansi.org/Shared%20Documents/Standards%20Activities/American%20National%20Standards/Procedures%2C%20Guides%2C%20and%20Forms/ANSI-Essential-Requirements-2018.pdf>

²³ A social trap is a situation where cooperation between individuals, groups, organizations, multi-stakeholders, or societies has become impossible due to mutual lack of trust. See note 3.

approaches that are more flexible and iterative. This lack of trust exists today, and will need to be actively overcome. Removing this obstacle should be a high priority for legislation and the FTC.

B. FTC Rulemaking

The FTC Operating Manual²⁴ 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,²⁵ 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

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

²⁴Federal Trade Commission Operating Manual, Ch. 7, Rulemaking, available at <https://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch07rulemaking.pdf>.

²⁵Administrative Procedure Act (APA), Pub. L. No. 79-404, 60 Stat. 237 (1946) (5 U.S.C. §§ 551–559, 701–706 (2012)).

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.²⁶ 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.²⁷ Notably, the FTC took 5 months to complete its 2009 Health Data Breach rule,¹¹ a rulemaking which WPF commented on.²⁸

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. If the FTC is not freed of this encumbrance, it does not seem likely that any privacy framework would be effective.

²⁶ 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.

²⁷ 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.

²⁸ World Privacy Forum, http://www.worldprivacyforum.org/wp-content/uploads/2009/08/WPF_FTCBreachcomments_06012009_fs.pdf

C. Scaling Knowledge Governance

Ostrom's governance system has been proven to scale from small ecosystems to large, complex ecosystems in other disciplines. For a knowledge governance system to work in the area of data and privacy, it would require the following things in order to happen:

1. Federal privacy legislation to set forth baseline privacy principles, such as FIPs.
2. Legislation to set forth broad governance guidelines to address the implementation of those principles. (Ostrom)
3. Legislation that sets forth specific due process rules for creating specific principles in areas of the data ecosystem which are determined to present enhanced privacy risks. (Such as WTO or *ANSI Essential Requirements*.)
4. Legislation that allows the FTC to enforce the new rules for due process in creating standards, in an oversight capacity, while at the same time not requiring the FTC to participate in every process.
5. An environment where problems associated with widespread mutual mistrust between privacy stakeholders (social traps)have been resolved. If the FTC had authority to step in when a stakeholder or stakeholder group did not follow established rules for due process for creating principles, this would end the situation where companies and trade associations or other groups simply create principles and then announce them to the world. Trust could eventually be established in such an environment.
6. It would be helpful if creating principles without consulting stakeholders, or doing other things that violated the rules, would be considered to be an unfair and deceptive act or practice.
7. Individuals as a stakeholder group will need a meaningful seat at the table. Principles creation without all stakeholders is not viable or sustainable in the long run.
8. These processes should be iterative and learn from advances and mistakes.

A repeat of the warning: the Ostrom governance principles are quite different from what is often called risk management today. Risk management does not include the concept of mutuality often, if at all.

III. Privacy Case Studies: Data brokers, AI and machine learning, Biometrics

We note that most of the US federal legislative proposals thus far have set forth a variety of well-understood principles and mechanisms. To highlight where some key problems are, and focus on solutions, we are setting forth three case studies that highlight significant and challenging modern privacy issues that have not yet been fully addressed by legislation or proposed legislation.

A. 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.²⁹ Nowhere has this deficit been more problematic than in the data broker industry. Economics scholars have articulated the secondary use problem as “data poaching,” and describe it as one of the transactional risks of data ecosystems.³⁰ The World Privacy Forum has spent years researching and documenting data broker practices that impact at the individual level, and has found that secondary uses of data by data brokers can cause much economic impact and other marketplace and life impacts for individuals.³¹

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.³² Thousands of data broker lists exist, with millions of consumers identified in the lists by name.³³
- 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.³⁴

²⁹ The state of Vermont enacted the nation’s first data broker law in 2018. The statute defines data brokers as: a data broker is defined as: “a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.” See: See: H.764, An act relating to data brokers and consumer protection. <https://legislature.vermont.gov/bill/status/2018/H.764>

³⁰ Eric K. Clemons and Lorin M. Hitt, Poaching and the Misappropriation of Information: Transaction Risks of Information Exchange. *Journal of Management Information Systems*, Vol. 21, No. 2, Competitive Strategy, Economics, and Information Systems (Fall, 2004), pp. 87-107. <http://www.jstor.org/stable/40398693>

³¹ See World Privacy Forum work on data brokers — Reports: *The Scoring of America*, *Data Brokers and the Federal Government*, *The One Way Mirror Society*. See also: *Top Ten Opt Outs*, *Data Broker Opt Out List*. See also: WPF Congressional Testimony regarding data brokers and privacy from 2009, 2013, 2015. Available at worldprivacyforum.org

³² See World Privacy Forum, Congressional Testimony Page: <https://www.worldprivacyforum.org/category/congressional-testimony/>.

³³ See Nextmark List Finder, <https://lists.nextmark.com/market>. The List Finder is a search engine for data broker lists.

³⁴ For a recent article about Consumer Lifetime Value scores, see: Khadeeja Safdar, *On hold for 45 minutes? It might be your secret consumer score*. *Wall Street Journal*, Nov. 1, 2018. <https://www.wsj.com/articles/on-hold-for-45-minutes-it-might-be-your-secret-customer-score-1541084656>.

- 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.
- It is not feasible or even possible for individuals to “opt out” of all data broker activities. First, not all data brokers offer opt outs. Even if all data brokers allowed for opt-outs, doing so places an unwelcome and impossible burden on consumers. People who have used the WPF data broker opt out list have told us that it takes about one week to opt out of the major data brokers who offer opt outs.³⁵ From our experience, it also take follow-up work. Most consumers do not know about data brokers. How can we reasonably ask consumers to simply opt out as a primary solution? This is unreasonable and impractical, and does not fundamentally solve the problem.

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:

- A knowledge governance process, based on principles devised by all stakeholders, where individuals have a seat at the table. This is ultimately much more powerful than individuals being given the choice at the end of the line to opt out, consent, click, check a box, or other such mechanisms. The real power for consumers is in having a voice throughout the entire decisioning process in principles and specific aspects of governance.
- Creating actual transparency, 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.
- Companies that use data broker products should also be subject to standards, and should have transparency requirements.

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.

A frequently proposed solution in the consumer data privacy space is to grant individuals more control of their data. This sounds, in theory, wonderful. And in some circumstances, it is the right

³⁵ Conversations with WPF executive director Pam Dixon at NNEDV SafetyNet trainings.

thing. But applying these ideas to data broker activities reveals how this approach becomes unmanageable in many ways. We have considered the impossible burdens of opting out in a complex data ecosystem. Let us look at an additional popular idea, for example, one that the NTIA (and others) have proposed, that users would have 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.³⁶ We also know that data brokers share with retailers intimate details of consumers based on their debit and credit card information.³⁷ 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, among other acquired or inferred 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.

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.³⁸ This should be the goal.

How does user control work in complex data broker circumstances? The best parties to determine the answer to this and other questions are the stakeholders involved. It may be necessary to create principles at a company-by-company basis. Smaller ecosystems can be managed with more specificity and stakeholders can arrive at solutions that are iterative and provide all parties with the

³⁶ See 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/>.

³⁷ See the roster of lawsuits by Stonebarger Law relating to California's Beverly-Song Act, one of which rose to the California Supreme Court, *Pineda v. Williams Sonoma*, Available at: <https://law.justia.com/cases/california/supreme-court/2011/s178241/>, The lawsuits have revealed many interactions between retailers, data brokers, and payment methods. See also *Hernandez v. Restoration Hardware* Available at: <https://law.justia.com/cases/california/court-of-appeal/2016/d067091.html>.

³⁸ See for example, Centers for Disease Control data sets: <https://www.cdc.gov/nceh/data.htm>.

ability to achieve benefits and goals.³⁹ But there has to be a governance mechanism that facilitates achieving these outcomes, and there has to be an understanding that individual consumers are part of the process all along, and not relegated to check box management at the end with no real voice in the matter. That era needs to end. The data broker problem is one that needs to be solved. Unrestrained data uses are not sustainable over the long term, particularly as people become aware of data broker practices and increasingly lose trust in those entities (including in some cases retailers) that pass data along for secondary uses or that use information acquired from data brokers in ways that can have meaningful impacts on individuals' lives.

B. 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 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 in the past few years 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. We would like to pause here and support Japan's AI Guidelines, which in 2018 are now a completed draft after substantive multistakeholder deliberation.⁴⁰ The guidelines are thorough, fair, and balanced. To date, these are the most thorough and balanced general guidelines on AI.

Two tension points in particular are often overlooked, and we want to highlight them here. That is, **input risks**, and risks regarding **interpretation and use of results**. We focus on these two areas here.

³⁹ See, generally, the work of Elinor Ostrom. [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.

⁴⁰ *Draft AI Utilization Principles 17 July 2018*. Japan. The Conference Toward AI Network Society. http://www.soumu.go.jp/main_content/000581310.pdf. These guidelines were crafted with multi-stakeholders and inclusive of Ministry-level experts, academics, and others. The Guidelines were crafted over several years.

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 privacy 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 what has been proposed 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. “Risk mitigation” is not the same as a full knowledge governance system, which also articulates risk, but also creates solutions with mutuality and all stakeholders involved with rules that create due process and non-dominance.

The NTIA model, and in fact most models, do not fully address consent and transparency of use — it is simply not possible for some AI 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 and the need for privacy assessments for enhanced risks) 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 - and other privacy frameworks — often deal 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, and does not produce a sustainable or useful path forward. Specific governance will be required, and will need to be constructed for use cases as required by ongoing risk analysis and responsiveness to problems.

Regarding interpretation and use of AI outputs

How to interpret the results of AI analysis also 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 and use of specific 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 in the area of use of AI scores or models.

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

Principles proposed for federal privacy legislation that articulate 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. In the past, individuals are not given a seat at the table and there has not been oversight over how principles are created at the ground level.

Moreover, data transformation must be addressed. By leaving data transformation out of the “data provided” idea, 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.

C. Biometrics and data governance

Biometrics has become a popular topic of debate in privacy. In the US, there is a great deal of interest in creating some form of individual control over biometrics use. At least one state, Illinois, has a state-level law mandating consent prior to use.⁴¹ Some groups have proposed general principles for biometric deployment and use, and some have proposed bills. Currently, the principles often reflect narrow bands of a few selected stakeholders, resulting overall in competing ideas that meaningfully diverge. Some principles have been crafted with corporate goals in mind, some have been crafted with privacy goals in mind from a consumer point of view. However, none of the governance-focused biometric ecosystem principles have been created according to, for example, the due process requirements set forth in the ANSI *Essential Requirements*. (Non-technical principles.)

With the lack of mutual trust in biometrics and the lack of a meaningful dialogue between all stakeholders, it will be very difficult to craft a legislative approach or governance that is responsive to the full range of stakeholders.

India, which has provided the world's most significant case study on the implementation of nationwide biometric systems in voluntary and non-voluntary environments, provides important lessons to be applied here. WPF researched the Aadhaar ecosystem extensively, and wrote a large research report on the system.⁴² Our research was cited twice in the Supreme Court of India's landmark Aadhaar case, in 2018.⁴³

Why is any of this relevant to the US? It is relevant because Aadhaar, more than any other case study, shows us where the factual end stages of biometric deployment are, and what they look like and how they operate. The outer limits have been largely explored now, and the lessons are already there, including the loss of trust the Aadhaar system experienced.

India went from adding its first voluntary 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

⁴¹ Biometric Information Privacy Act (760 ILCS 14/) Available at: <http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57>

⁴² 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/>.

⁴³ Aadhaar case: Supreme Court of India, Justice K.S. Puttaswamy (Retd.) and another v. Union of India and others. Writ Petition (Civil) No. 494 of 2012. Decided Sept. 26, 2018. Available at: <http://www.worldprivacyforum.org/wp-content/uploads/2018/09/Supreme-Court-Aadhaar-Judgment-26-Sep-2018.pdf>

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 by the 2018 Aadhaar Supreme Court of India decision.

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. Three factors: the lack of stakeholder input, mission creep, and eventually a loss of user trust in the system, are what truly caused the curtailment of Aadhaar.⁴⁴

Regarding potential federal biometric legislation and creation of governance principles in the US, key lessons may be drawn. 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 is a major lesson from Aadhaar; scale must be considered when answering any question balancing innovation and restriction of technology. Outlining concerns as well as duties for all stakeholders would have gone far to preventing some of the worst of the mission creep in Aadhaar.

Another lesson for the US is that all biometric 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 mutuality. This means actual dialogue with user stakeholders and giving stakeholders appropriate voice. Bills or rules created by dominant actors in an environment without mutual trust and dialogue will not be sustainable over the long term.

Creating principles of data governance with mutuality is extremely important for any federal biometric legislation. Government systems will likely continue to be governed by the Privacy Act. Commercial systems will likely need federal legislation, and that legislation, to be effective, will need to provide the elements discussed at length in these comments regarding a structure inclusive of FIPs plus governance that includes due process and non-dominance, with FTC oversight of any principles process.

⁴⁴ There were additional issues related to 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 people who could not get food. In India, there were reports of people dying because of failures to authenticate. 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>

Governance will be needed to address the roles of stakeholders, and responsibilities and duties of stakeholders. This will be an important aspect of any guidance.

In situations where biometric collection and use of data is either non-voluntary, or becomes too complex to get granular consent, creating multi-stakeholder principles is essential. In biometrics, it can become extremely difficult to get consent. But what will this mean in practice? Do we accept lesser freedoms, or do we impose stricter privacy controls? Is there another pathway? A formal standards - principles setting process such as articulated by the WTO procedures or the ANSI *Essential Requirements* would allow all stakeholders to build trust and craft mutually acceptable rules. This would not be easy. But it is necessary.

IV. 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.

Command and control regulation does not work with the complex and volatile structure of modern data environments. Simple check boxes are not where the power is. We have been so busy thinking about opting in or opting out, that somehow, we all missed that privacy — real privacy — lies elsewhere.

There is an important window of opportunity right now to act on federal privacy regulation, and solve for the privacy problems that we are regularly seeing writ large in headlines.

The era of technology chiefs proclaiming that “privacy is dead” has now passed by. No one credibly believes this anymore. People care about their privacy, and they want it. But the old controls and mechanisms have frequently led to deep disempowerment of individuals. Taking back fairness and power means an appropriate distribution of voice, a seat at the table, and real rules for creating mutually-agreed upon rules, with the FTC having the power to veto any rules that are created without following the playbook.

We need good privacy principles, but we also need solid knowledge governance. If we get privacy legislation without a way to achieve proper knowledge governance, then privacy problems will not have been adequately addressed. Privacy principles plus knowledge governance inclusive of due process will help solve the existing problems of lack of trust. (Social traps).

The case study of data brokers is the one we end these comments with: consumer trust and data brokers, and to some degree biometrics, are the proverbial canaries in the coal mine: if the privacy legislation envisioned at the federal level does not articulate a solution to the data broker problem that provides a pathway out of social traps, nor to the same with the impending biometrics problem, then we will know by these tests that the legislation will not have done its job.

We thank the FTC for its attention to these matters of crucial importance, and we stand ready to discuss these challenges with the FTC and to help wherever we can. We submit these comments in a spirit of hopefulness that there is indeed a pathway forward that can be more effective.

Respectfully submitted,

S/

Pam Dixon
Executive Director,
World Privacy Forum